DataSMART® 696/698 T1 FrameVision™ DSU/CSU User's Guide

72696 DataSMART 696, FrameVision DSU
72698 DataSMART 698, Add/Drop FrameVision DSU

Document #5000161

KENTROX®
A Platinum Equity Company

Copyright

Specifications published here are current or planned as of the date of publication of this document. Because we are continuously improving and adding features to our products, Kentrox reserves the right to change specifications without prior notice. You may verify product specifications by contacting our office.

In no event shall Kentrox be liable for any damages resulting from loss of data, loss of use, or loss of profits. Kentrox further disclaims any and all liability for indirect, incidental, special, consequential or other similar damages. This disclaimer of liability applies to all products, publications and services during and after the warranty period.

Trademark information

Kentrox and DataSMART are registered trademarks of Kentrox, LLC.
FrameVision is a trademark of Kentrox, LLC.

All other product names are trademarks or registered trademarks of their respective owners.

Revision history

Part #	Date	Description
65-72696101	November, 1998	Issue 1
5000161	December, 2001	Issue 2

Contents

Chapter 9 Troubleshooting

Preface

This manual contains a detailed description of all operations of the DataSMART 696 and 698 Data Service Units (DSUs). It provides specific information for configuring the DataSMART units and for using them to monitor and troubleshoot your T1 and Frame Relay circuit's performance. It also provides detailed listings of all DataSMART menus, commands, and specifications.

Who should read this manual?

This manual is intended as a reference source for ongoing operation of the DataSMART 696 and 698 DSUs. It covers all possible operations and configuration choices in detail. For initial installation, power up, and basic configuration of the units, we recommend that you first turn to the *DataSMART 696 and 698 Installation Guide*. Note that installation and service should be performed only by trained and qualified personnel.

Viewing this manual as a PDF file

This manual is designed to be used as both a printed book and a PDF file, and includes the following features for PDF viewing:

- Cross-references are clickable hyperlinks that appear in blue text.
- Chapters and section headings are represented as clickable bookmarks in the left-hand pane of the Acrobat viewer.
- Page numbering is consistent between the printed page and the PDF file to help you easily select a range of pages for printing.

You can obtain PDF files of our manuals by visiting http://www.kentrox.com.

Related publications

In addition to this manual, the following are available:

- *DataSMART 696 and 698 Installation Guide*
- *Kentrox DSU/CSU MIB Reference*, available in our World Wide Web online library at http://www.kentrox.com

MIB source files

The MIBs and software updates are available by visiting: http://www.kentrox.com/support.

Conventions used in this manual

This manual employs the following conventions when explaining command-line syntax:

Literals	Bold type identifies commands and syntax elements that must be entered exactly as shown in the text.
Variables	Italic type identifies variable syntax elements, such as values or alphanumeric strings you can enter.
x|*y*	A vertical line between elements means that the elements are mutually exclusive; you can select one and only one of the elements.
[ ]	Brackets indicate items that are optional.

Who to call for assistance

If you need assistance with this product or have questions not answered by this manual, please visit our Support page on the Kentrox Web site. You are also welcome to call or send email to our Technical Assistance Center. Please have your product's software revision and hardware serial numbers available to give to the Support representative. All product returns must include a Return Authorization number, which you can obtain by calling the Technical Assistance Center.

The numbers listed below are current at the time of publication. See the Kentrox Web site for detailed contact and warranty information.

1-800-733-5511 (continental USA only)
1-503-350-6001
email: support@kentrox.com
http://www.kentrox.com

C H A P T E R

1 *Introduction*

The DataSMART Model 696 and 698 FrameVision Plus data service units (DSUs) monitor physical-layer and frame-level performance of your T1/FT1 Frame Relay service. They connect routers, Frame Relay assemblers/disassemblers (FRADs), and other customer premise equipment to the network.

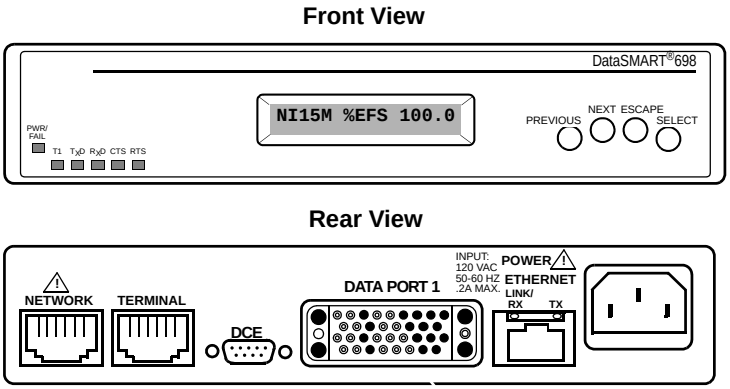
You can use SNMP to manage the units remotely via one or more of these methods: Frame in-band management through the T1 network interface or through the data port, via the Ethernet port, or using the SLIP protocol on a control port.

This user's guide covers two DataSMART configurations:

- The Model 696 DSU, with one data port and an Ethernet port
- The Model 698 add/drop DSU, with one data port, an Ethernet port, and a terminal interface

Both models are housed in the same one-unit-high (1 RU) rack-mount box.

Figure 1—The DataSMART front and rear panels



Features of the DataSMART

A front-panel interface for easy installation

- LCD and pushbutton interface can be used to completely configure a DataSMART
- Intuitive interface simplifies troubleshooting

IP-based network management (all units)

- You can configure, monitor, and troubleshoot individual units using standard network management tools
- IP interface generates traps when network events occur
- Unit responds to pings
- IP interface allows Telnet access
- Unit supports MIB II (for LAN-based hosts), the DS1 MIB (for T1 line management), and an Enterprise MIB (which allows SNMP access to all commands available via the control port menu interface; this includes performance monitoring, diagnostics and reconfiguration).

Options for IP management connectivity

- In-band access is available via Frame Relay
- Ethernet access is available via a 10Base-T connector
- Serial-port access is available via the asynchronous serial connection (DCE port) using SLIP protocol

T1 performance monitoring

- Reports show details of T1 interface performance
- Unit retains T1 summary report data for seven days while powered up
- Unit provides detailed terminal interface reports (add/drop units only)

T1/Frame diagnostics

- LEDs and front-panel display indicate problems at the network interface, data port, and Ethernet interface
- LEDs and front-panel display indicate problems at the terminal interface (add/drop units only)
- Unit allows T1 access loopbacks to be set remotely or locally
- Automatic Frame Ping (FPING) establishes end-to-end VC connectivity and measures round-trip network delay
- User interface shows real-time status of system

Frame monitoring features

- Virtual Circuit Utilization Report compares each virtual circuit's bandwidth usage to

its Committed Information Rate (CIR) and Excess Information Rate (EIR)

- VC performance reports provide both a summary of the performance of all configured VCs and details of a single VC
- Frame Relay statistical report counts unusual network events
- You can set thresholds for end-to-end network delay and total access link bandwidth utilization
- Unit retains frame summary report data for seven days while powered up

Security features

- IP source address screening rejects IP packets from unauthorized hosts
- Telnet password provides security for remote logins
- Authentication traps report failed Telnet login attempts, SNMP community strings, and IP packets received from invalid IP hosts
- Control port access protected by three levels of user password
- LCD access password protects unit from unauthorized access to front panel
- LCD operates in read-only or read/write mode

Nonvolatile memory

- Retains unit's configuration for five years minimum without power

CHAPTER

2 *Entering commands and logging in*

This chapter describes:

- Entering commands via the command-line interface
- Entering commands via the front-panel interface
- Logging into the DataSMART

Using the DataSMART

With the command-line interface you use a terminal to manage and monitor the DataSMART DSU.

Using the command-line interface

The DataSMART command-line interface is accessible through various physical connections:

- Telnet via the Ethernet 10Base-T connector
- Telnet in-band over the T1 or V.35 connection to a frame-based service
- Telnet via a SLIP connection to the unit's DCE control port
- ASCII (non-IP) connection to the control port

Menus vary according to your DataSMART model. Some commands apply only to the DataSMART 698 add/drop unit.

Figure 2—The Main Menu

```
        DataSMART 698 Version 1.nn Copyright (c) 1998 Kentrox
                      NAME: PORTLAND,OR

MM                      - Main Menu
SS                      - System Status
R                       - Reports Menu
RFRM                    - Frame Relay Monitoring Reports Menu

LM                      - Local Maintenance Menu
RM                      - Remote Maintenance Menu

AC                      - Alarm Configuration Menu
CC                      - Control Port Configuration Menu
DC                      - Data Port Configuration Menu
FC                      - Fractional T1 Configuration Menu
FMC                     - Frame Management Configuration Menu
MC                      - Management Configuration Menu
NC                      - NI Configuration Menu
PC                      - Password Entry and Configuration Menu
SC                      - System Configuration Menu
TC                      - TI Configuration Menu
^D                      - Logout

MM>
```

DataSMART 698 only

To see the System Status menu, enter **SS** at the prompt.

```
                SYSTEM STATUS

ARC/DRC         - Access to/Disconnect from Remote Unit Control
S               - System Status Screen Command

SSV             - View System Setup
```

To see system status, enter **S** at the prompt. See "Examining system status" on page 139 for more information on operational status of the DataSMART.

Use the **SSV** command to see all the configured parameters for your unit. This displays the configuration for every menu.

To see one of the menus, enter the menu name at the prompt. For instance, to see the Reports menu, enter **R** at the prompt.

DataSMART 698 only

DataSMART 698 only

```
MM> R
                    REPORTS MENU

UNSR / UNLR      - User NI Short/Long Performance Report
UTSR / UTLR      - User TI Short/Long Performance Report
FESR / FELR      - Far End PRM Short/Long Performance Report
NSR:[z]          - User NI Statistical Performance Report
TSR:[z]          - User TI Statistical Performance Report
                   z = Display Report, then Zero Counts (Optional)
AHR              - Alarm History Report
SHR              - Security History Report

PL:<len|style>   - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                   <style> = P (Page Break), M (More), or V (View)

R>
```

Each time you change menus, the command-line prompt changes to indicate which menu is current. In the preceding figure, the first line shows a prompt of “MM>” meaning that the Main Menu is current. However, once **R** is entered and the Reports menu is displayed, the prompt becomes “R>”, indicating that the Reports menu is current.

The current menu displays when you press the Enter key. In normal use you are likely to use a series of commands from a given menu, and so you can make that menu current and get a menu listing whenever you need it by pressing the Enter key. However, you may enter any command at the command line, even if it is not on the “current” menu.

Command-line syntax

A typical command line consists of the command and zero or more arguments, all separated by one or more delimiters. The following are all valid delimiters: a space, a tab, a comma, a colon, a forward slash. You can use any combination of valid delimiters to separate arguments.

For example, **SD 12/08/98** and **SD 12 08 98** are both valid commands to set the date to December 8, 1998. However, SD 12-08-98 is not, because the dash is not a valid delimiter.

When entering an IP address or netmask, follow the dotted decimal convention (i.e., *nnn.nnn.nnn.nnn*) and include periods as part of this ID. The DataSMART will interpret the ID as a single argument.

There is an exception to these rules, a string value entered for the **SN, TCS**, **RCS**, **WCS**, **TPW**, **EPS**, **APS**, or **DPS** commands. In a string value, a space, comma, forward slash, or colon can appear in the argument, as long as there is a non-delimiter preceding it somewhere in the string. For example, this is a valid instance of the **SN** command:

SN PORTLAND, OR

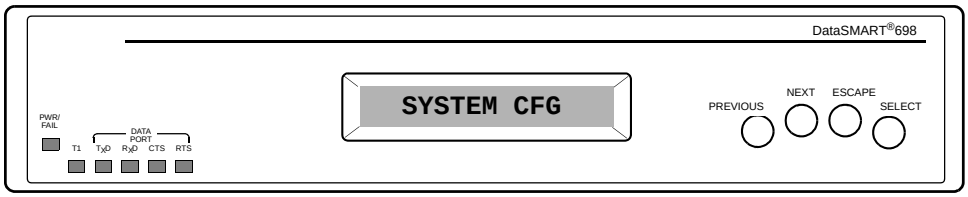
Type-ahead

You may enter the next command while a previous command is executing.

Using the front-panel interface

The front-panel interface is modeled after the command-line interface and provides most of the same functionality. The front-panel interface uses a hierarchical structure that you traverse using four pushbuttons on the front panel to find the command you need. The LCD display provides the visual readout.

Figure 3—The LCD display and pushbuttons



The hierarchical levels of the front-panel interface correspond to the menus, commands, and command options of the command-line interface. The main menu at the top of the hierarchy corresponds to the Main Menu of the command-line interface. Below that, depending on the complexity of the command, submenus correspond to the command menus of the command-line interface, then further subtrees allow you to select command options.

Traversing the menu hierarchy

The Select button moves you deeper into the hierarchy, the Escape button moves you back out towards the top. The Next or Previous buttons cycle you through all elements in one level of the hierarchy.

The figure on the next page illustrates these rules.

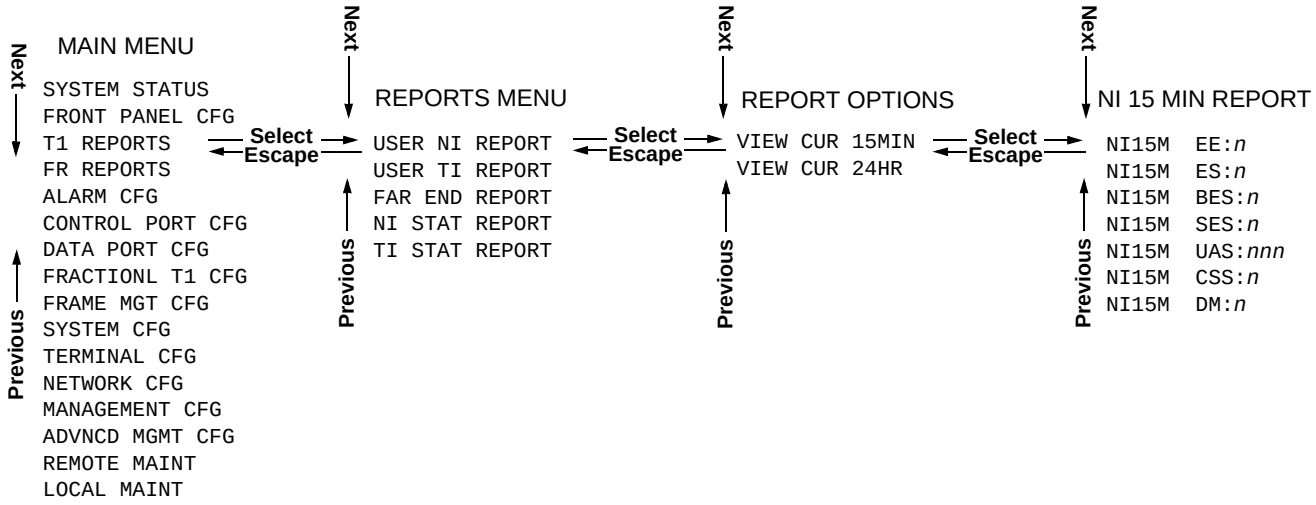
1. The Main Menu is on the left side of the figure. Push Next or Previous to cycle through the items on the Main Menu. When you see the item you want, push Select to descend to the next level, in this case the Reports menu.

2. In the Reports menu, push Next or Previous to cycle through the report choices. When you see the report you want, push Select to descend to the next level, the Report Options.

3. From the Report Options menu, choose to view either the report for the current 15 minutes or the current 24 hours; then push Select to descend to the first item in the report display.

NOTE

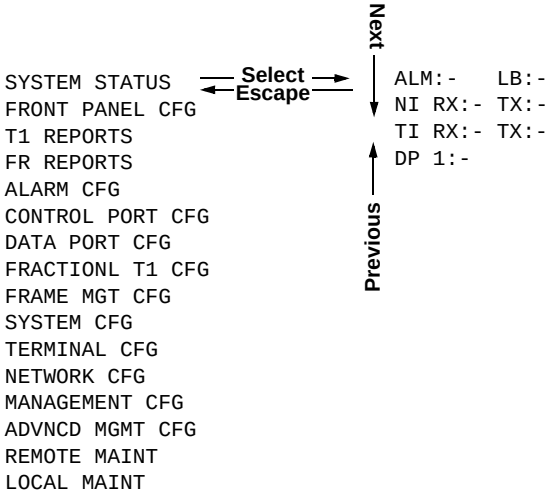
The TERMINAL CFG command and TI reports are available on add/drop units only.



Notice that you can "cycle" through items at each level in the hierarchy, and yet there is a conceptual "top" to each. Each level is circular in that pushing Next or Previous eventually brings you back to where you started. Each level has a "top" in that whenever you descend to a level by pushing Select, you always see the top item in the level. In the case of the Reports menu, the top item is USER NI REPORT.

However, when you use Escape to ascend from one level to the one above, you go back to the item that you originally descended from. For instance, if you entered the Report Options menu from FAR END REPORT, you would return to FAR END REPORT if you pushed Escape.

Not all hierarchies in the front-panel interface are as complex as the one in the last example. For instance, the simplest is for reading the System Status. In this case, when you see SYSTEM STATUS in the display, push Select. You can then use Next or Previous to cycle through the System Status display.



NOTE

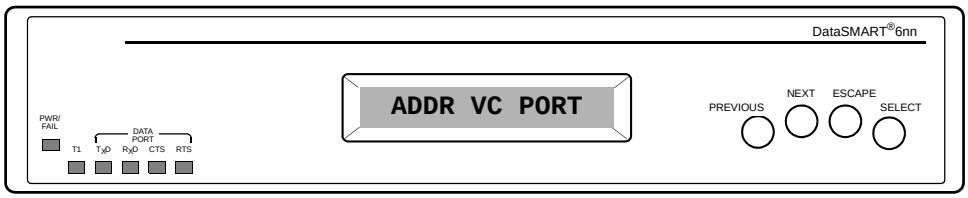
If you lose your place in the hierarchy, you can always return to a known point by pushing the Escape button until you see SYSTEM STATUS in the display; you will be back at the top of the Main Menu.

Using the front panel for entering values

You can use the front panel for configuring ports, channels, and performing other operations that require you to enter values. There are three basic situations when entering values:

- Selecting from multiple choices displayed together in the panel
- Selecting multiple choices by cycling through a list
- Entering a string, IP address, or channel configuration

Selecting from multiple choices displayed together. The figure below illustrates choices displayed together.

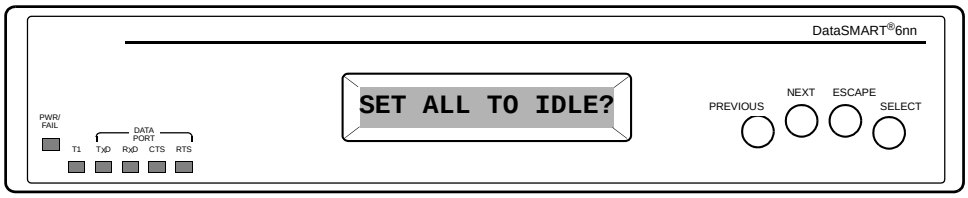


When the display appears, the current selection is blinking. To change to another value in the display, push Next or Previous. As you cycle through the selections, each will blink in turn.

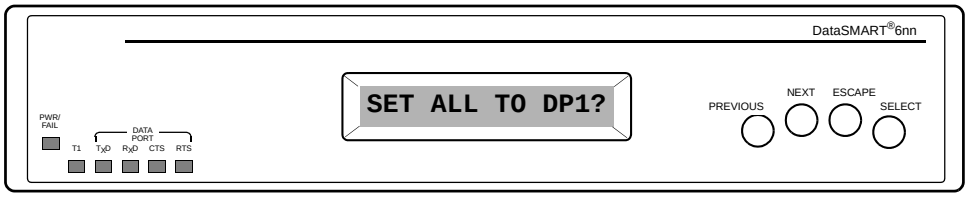
TIP
When you change a setting in the LCD display, a question mark appears indicating that a change to the DataSMART configuration is pending. Push Select to accept the changes; push Escape to return the display to the original setting with no change to the configuration.

As soon as you change a selection in the display, a question mark appears on the right side of the display, indicating a change has been made in the display that has not yet been saved to the DataSMART configuration. Push Select to make the change to the configuration and the question mark disappears (except in the case of entering a string, IP address, or channel configuration. See page 20.)

Selecting multiple choices by cycling through a list. In this case, you cannot see all your choices in the display. For example, the following figure shows a display for fractional T1 configuration. In the display, “IDLE” blinks to indicate that it is the current selection and can be changed.

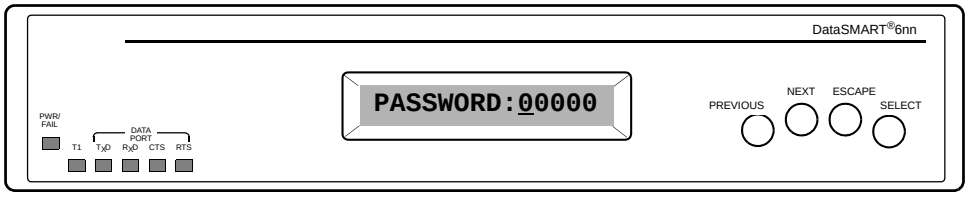


Pushing Next changes the selection to “DP1” as shown below. The question mark indicates that a change to the configuration is pending. If you push Select now, DP1 will become the current configuration.



Entering a string, IP address, or channel configuration. The figure below illus-

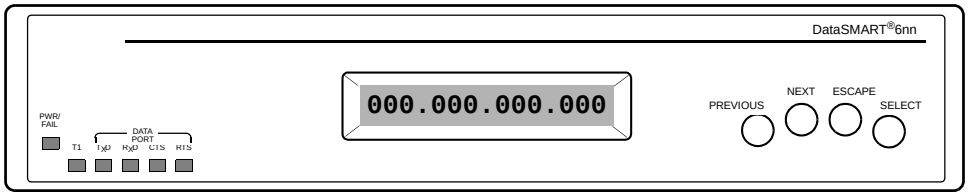
trates the display for changing the front-panel password. As the figure shows, a password is a string of six numerals.



When the display first comes up, the first numeral is underlined. Pushing Next or Previous moves the underline to a different numeral. To change the underlined numeral, push Select. The underline disappears and the numeral begins blinking. When the numeral is blinking, push Next or Previous to change the value (0-9).

As soon as you change the numeral in the display, a question mark appears to the right, indicating that you have changed a value in the display but have not yet saved the value in the DataSMART configuration. Push Select to make the change to the configuration. The numeral stops blinking, the question mark disappears, and the underline reappears. You can now use Next or Previous to move the underline to a different numeral for further editing. If you push Escape when the question mark is showing, the numeral returns to its original setting.

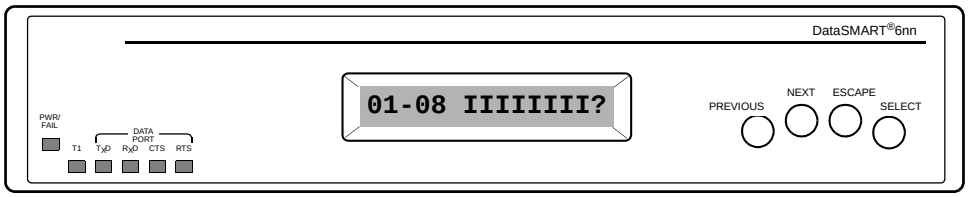
Entering an address works similarly, though with some differences worth noting. For instance, the following figure shows the display for setting the IP address. In this case, Next or Previous moves the underline between the fields rather than stopping at each numeral. You use the same procedure to change the fields as for changing the numerals of a password.



The question mark appears each time you edit a field, and disappears when you push Select. However, the changes you make in the display do not take effect in the DataSMART configuration until you leave the IP address display. In other words, after you make all the changes to the fields (pushing Select after each one), you must push Escape. The query SET NEW ADDRESS? appears in the display. If you push Select, the changes are made to the configuration. If you push Escape, the changes you made in the display are discarded.

The process for entering channel configurations has similarities to both entering strings and entering addresses.

The following figure shows the initial channel configuration display. The display shows the settings for channels one through eight, which in this case are all set to idle, as indicated by an “I” for each channel.



When you first enter the display (from the Fractional T1 Configuration menu), the channel range is blinking. If you push Next or Previous at this point, the ranges will cycle through “01-08,” “09-16,” and “17-24.” When you see the range you want to edit, push Select. The range will stop blinking, and an underline will appear under the token representing the first channel.

At this point, you change the token just as you would change a numeral in the password string. Push Select, and the token begins blinking, then push Next or Previous to change the token. The question mark appears when you change the token. When you have changed the token to the one you want, push Select; the question mark disappears and the underline reappears. You can then use Next or Previous to move the underline to the next token you wish to change.

Once all the channels for the range are correctly set, push Escape. The range begins blinking and you can change to the next range. When all the channels are set correctly, push Escape to exit the channel configuration display. The query “LOAD NEW CHANS?” appears. Push Select to load the new channel configuration into the hardware or push Escape to discard the changes.

Logging in

You can log into a DataSMART unit using an ASCII connection to the control port or using IP access through an Ethernet port. Passwords are not needed, but when implemented, can restrict some users from using some commands.

The DataSMART can be accessed through a number of methods:

- Using the command-line interface over an ASCII connection to the unit's DCE control port
- Using the command-line interface over an IP connection (Telnet) to the Ethernet port
- Using the command-line interface over an IP connection (Telnet) to the control port, configured for SLIP
- Using the command-line interface over an IP connection (Telnet) in-band over the T1 or V.35 connection to a frame-based service
- Using the front-panel LCD interface
- Using an SNMP network manager over an IP connection

In general, a password is not needed to log into a DataSMART unit. Though DataSMART units support passwords, the passwords do not prevent login but instead restrict users from executing various commands. (See Chapter 3 for procedures on setting passwords.)

Depending on whether you are accessing the DataSMART through Telnet, in-band via Frame Relay, or the DCE control port, the procedure for logging in differs.

Through the control port via ASCII

On the command-line interface, press the Enter key to log in. The DataSMART unit will display the Main Menu and the command prompt, indicating you are logged in.

Telnet access

If your DataSMART unit has been configured for IP access and you have set up a Telnet password on the unit, you can log into it using Telnet. When you enter the unit's IP address and attempt to log in, you will be prompted for its Telnet password. If the DataSMART has not been set up for IP access and assigned a Telnet password, you will not be able to log in.

See Chapter 6 for information on configuring a DataSMART unit for Telnet login.

Logging out

You should always log out of the DataSMART when you are done.

To log out, enter ^**D**. (Press the Ctrl and D keys simultaneously.)

NOTE
No message will appear to indicate that you are logged out.

You can also log out by disconnecting the control port cable.

The DataSMART has an auto-logout feature that logs you out after a period of inactivity. Auto-logout is always enabled when Telnet is being used. If auto-logout was disabled before a Telnet session is started, auto-logout is set to 15 minutes for that Telnet session. When the user logs out, auto-logout reverts to the default configuration value. If auto-logout is enabled before a Telnet session is started, the auto-logout time will not be changed. See "Setting auto-logout for the control port" on page 38.

CHAPTER

3 *Establishing system security*

In order to prevent unauthorized users from changing the system configuration, setting loopbacks, or performing other operations that might disrupt service, you need to secure access to the user interfaces.

This chapter shows you how to secure access to:

- The command-line interface via the control port
- The front-panel interface via the LCD and push buttons

The SNMP and Telnet security features are discussed elsewhere in this manual. For information about securing SNMP access, see “Setting SNMP community strings” on page 90 and “Using SNMP traps” on page 94. For information about securing the Telnet password, see “Securing your Telnet password” on page 81.

Securing the command-line interface

Security for the command-line interface is achieved through a system of passwords and privilege levels. Any user can access the command line without entering a password. But in order to gain a specific privilege level, the user must enter a password that has that privilege level assigned to it.

Restricting access

By default, there are no restrictions on which commands you can run on the DataSMART, and every user has super-user privileges. In order to restrict access, you must create at least one password with the super-user privilege level. Once you do, every user is restricted to the read-only privilege level unless they enter a password that permits more extensive privileges. You may create up to ten passwords (assuming you have super-user privileges) and assign them any privilege level you like.

NOTE

If you do not create a password with a super-user privilege level, every user that accesses the command line will be granted super-user privileges, regardless of whether or not you have created passwords for the other privilege levels.

Table 1—Privilege levels

Privilege level	Description
Read-only	Users with no password, and thus no privilege level, have read-only access. They can view menus, status screens, and performance reports, but they cannot execute any diagnostics nor change any configuration options.
Maintenance	Users with this privilege level can execute diagnostic tests, such as loopbacks and BERTs. Their activities can potentially disrupt data traffic through the device.
Configuration	Users with this privilege level can execute all tests allowed at the Maintenance level, plus they can change the configuration options of the DataSMART. Their activities can potentially disrupt service to the device.
Super user	Users with this privilege level have access to all commands allowed at the Configuration level, plus they have access to the commands that set up and control passwords.

The commands available for setting up and controlling command-line passwords are listed in the Password Entry and Configuration menu. To display this menu, log into the desired unit, then enter **PC** at the command line.

```
         PASSWORD ENTRY AND CONFIGURATION MENU

EPS:<password>          - Enter Password
                          password = 6 to 12 characters

APS:<access>:<password> - Add Password
                          access   = SA - Super User
                                     CA - Configuration
                                     MA - Maintenance
                          password = 6 to 12 characters

DPS:<password>          - Delete Password
                          password = 6 to 12 characters, or * for all

PUV                     - View User Access Privilege
PCV                     - View Password Configuration
```

Adding a password

You create a new password by using the **APS** command. You must have super-user privileges. The command syntax is:

APS:*access***:***password*

access — Specify the privilege level you want linked to the password: **SA** (super user), **CA** (configuration), or **MA** (maintenance).

password — Specify the password you want added. The string can comprise from six to twelve ASCII printable characters. (If the string you enter is either too long or too short, you'll get an error message.) Passwords are not case-sensitive and trailing spaces are not truncated.

Up to ten passwords are allowed. If you attempt to enter an eleventh password, you will get an error message. To add another password, you must first delete an existing password.

Each password must be unique.

Deleting a password

You delete a password using the **DPS** command. You must have super-user privileges. The command syntax is:

DPS:*password*

password — Specify the password you want deleted. The string must match the password exactly, except for case. You can also enter the * wild-card character to delete all current passwords.

Entering a password

To gain the privilege level associated with a password, use the **EPS** command. No special privileges are required. The command syntax is:

EPS:*password*

password Enter the password. Passwords are not case-sensitive.

If you enter the password correctly, DataSMART responds with the message PASSWORD ACCEPTED. If you enter an incorrect password, it responds with the message PASSWORD DENIED.

Viewing a user's access level

If you are logged into the device, you can view your privilege level by using the **PUV** command. You do not need any special privilege level. You will receive one of the following messages:

"User has No Access Privileges"
"User has MA Access Privileges" (maintenance)
"User has CA Access Privileges" (configuration)
"User has SA Access Privileges" (super user)

If your password was modified during your current session (e.g., a super user deleted your password, then added it back with a different privilege level), the change will not become effective until the next time you specify the password with the **EPS** command.

Changes to a user's password or privilege level take effect only after the user has logged out.

Viewing the current passwords

You can view a listing of current passwords and their privilege levels using the **PCV** command. You must have super-user privileges.

An example listing is shown below. The left column lists the current passwords, the right column identifies the access privilege levels.

```
        VIEW PASSWORD CONFIGURATION

Password      Access
------------  ------
BROWNS        MA
JOHNSOND      CA
MITCHELLS     SA
```

Securing the front panel

After you have installed the DataSMART and are controlling it remotely, you may want to disable the front-panel LCD and pushbuttons. Disabling the front panel prevents unauthorized or careless users from changing the DataSMART configuration and disrupting service.

A disabled front panel can be used for examining status, performance, and configuration, but not for changing any parameters. One way to think of it is that a disabled front panel is in “read-only mode” while an enabled front panel is in “read/write mode.”

There are two approaches to disabling the front panel. You can disable the front panel without setting a front-panel password, or you can set a password and disable it.

If you do not set a password, any user can disable, then re-enable the front panel. This provides minimum security for times when you want to temporarily disable configuration access. For example, you might want to secure the front panel this way while you are viewing status, since this would prevent you from inadvertently changing a parameter while pushing buttons. However, for full security you want to set a password. If you set a password, only users who enter the password can re-enable the front panel once it has been disabled. The front panel can also be re-enabled by entering EFP via the command line interface.

Using auto-logout

Another benefit to setting a front-panel password is that you can employ the front-panel auto-logout feature. This feature automatically disables the front panel if there has been no user activity at the front panel for a specified period of time. The information displayed on the front panel then changes to a readout of %EFS (percentage error-free seconds) when the auto-logout occurs. The next user needs to enter the password to re-enable the front panel.

If a password has not been defined for the front panel, the auto-logout feature has no effect except to show the %EFS display.

Setting the front-panel password

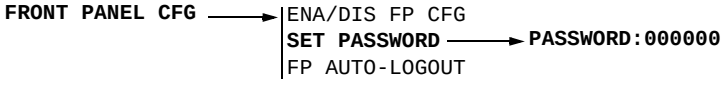
To set the front-panel password, use the steps shown below. The password is six digits. All zeroes is the equivalent of “no password.” Note that if the front panel is disabled, instead of seeing SET PASSWORD in the display, you will see ENTER PASSWORD.

The default password is 000000 (no password).

NOTE

If a password was previously set and then changed to no password (000000), the front panel will return to an Enabled state automatically.

The password is stored in the permanent nonvolatile configuration database.



1. When FRONT PANEL CFG appears in the display, push Select. ENA/DIS FP CFG appears in the display.
2. Push Next or Previous until SET PASSWORD appears in the display. Push Select. PASSWORD:0000000 appears in the display.

3 Push Next or Previous to move the underline marker to the digit field you want to change. Push Select. The digit will blink.

4 Use Next or Previous to change the digit value. When the digit is set to the value you want, push Select. The message PASSWD SET indicates that the password has been changed.

5 Repeat steps 3 and 4 to change the rest of the digits as desired.

Enabling/disabling the front panel

The default state for the front panel is enabled. The setting is stored in the permanent non-volatile configuration database.

To enable or disable the front panel when no password is set:

FRONT PANEL CFG → ENA/DIS FP CFG → ENABLE DISABLE

1 When FRONT PANEL CFG appears in the display, push Select. ENA/DIS FP CFG appears in the display.

2 Push Select. ENABLE DISABLE appears in the display, with the current selection blinking.

3 Push Next or Previous to choose the desired selection.

4 Push Select.

To enable the front panel when a password is set, you simply set the password. See "Setting the front-panel password" above.

Using the command line

You can also enable or disable the front panel from the command-line interface by using the **EFP** and **DFP** commands, respectively. You must have super-user or configuration privileges.

EFP Enable the front panel.

DFP Disable the front panel.

Setting auto-logout for the front panel

You can set the auto-logout timer to OFF (disabled), or from 1 to 60 minutes, inclusive. Use the steps shown below.

The default for auto-logout is OFF.

The auto-logout setting is stored in the permanent nonvolatile configuration database.

FRONT PANEL CFG → FP AUTO-LOGOUT → LGOUT TM: OFF
LGOUT TM: *n* MIN

The accepted values are 1 to 60 minutes, or OFF.

C H A P T E R

4 *Configuring the system*

This chapter discusses configuration operations that apply to the DataSMART as a whole. It covers the commands and options listed in the System Configuration, Control Port Configuration, and Alarm Configuration menus.

Topics include:

- Setting the DataSMART real-time clock and source clock
- Resetting the DataSMART unit to its default state
- Configuring the control port
- Configuring alarm message output
- Specifying error thresholds for reporting

For information on configuring interface ports and assigning channels, see Chapter 5.

For information on configuring the DataSMART for network management, see Chapter 8.

Specifying system parameters

You can control the system-level parameters and activities by using the command-line interface or the front-panel interface.

Command-line access

The commands for configuring the system parameters are listed below. To display this menu, first log into the unit, then enter **SC**.

```
                SYSTEM CONFIGURATION MENU

SD:<mm>,<dd>,<yy>   - Set Date (Warning: This also clears reports)
ST:<hh>,<mm>        - Set Time (Warning: This also clears reports)
SN:<id>             - Set Name
SMT/SMM             - Mode = Transparent/Monitor
EFP / DFP           - Enable/Disable Front Panel Operation
CLK:<src>           - Clock Source, src = L (Loop), I (Internal)
                      T (TI Rcv)
ALGOUT:<n>          - Autologout, n = 0..60 minutes
ZALL                - Zero All Counters used in User Reports
TSWDL:<i>           - Download program from a file via TFTP
                      i = n.n.n.n, n = 0..255 (dec), the
                          IP address of the TFTP host system
BOOT:               - Re-boot the system
WYV                 - View "What's Your Version" Information
RSD                 - Reset System to Default Values
SCV                 - View System Configuration
```

T option available on add/drop only

Front-panel access

The front-panel commands for configuring the system are as follows.

SYSTEM CFG →

- **SET DATE**
- **SET TIME**
- **SET NAME**
- **SET UNIT MODE**
- **CLOCK SOURCE**
- **AUTO-LOGOUT TIME**
- **ZERO COUNTERS**
- **VERSION INFO**
- **RESET DEFAULTS**

Viewing the current settings

Before changing any system parameters, you may want to look at the current settings. You do this by executing the **SCV** command. This command displays the View System Configuration screen.

```
        VIEW SYSTEM CONFIGURATION

Date          Time   Name             Autologout
------------  -----  ---------------  ----------
DEC 11, 1998  14:10  PORTLAND,OR      DISABLED

User Clock   Current Clock  Front Panel  Mode
-----------  -------------  -----------  -----------
LOOP         LOOP           ENABLED      TRANSPARENT
```

Field	Description
Date	This field displays the current date of the real-time clock.
Time	This field displays the current time of the real-time clock.

Field	Description
Name	This field displays the name assigned to the DataSMART unit you are logged into. The name appears in the Main Menu, in all performance reports, and in alarm messages. It is also the name returned for the MIB II *sysName* object.
Mode	This field indicates whether the unit is set for Frame Relay monitoring (Monitor mode) or for testing (Transparent mode).
Autologout	This field specifies the state of auto-logout. If auto-logout is enabled, it displays the auto-logout period in minutes.
User Clock	This field identifies the clock source you have assigned to be used as the system clock.
Current Clock	This field tells you the *actual* clock source being used as the system clock. Under normal operating conditions, this field will be identical to the "User Clock." If the unit loses its assigned clock, it switches to its internal clock.
Front Panel	This field tells you if the front panel is currently enabled or disabled.

Setting date and time

The DataSMART uses an internal, real-time clock to time stamp event occurrences. The time stamps appear in alarm messages and performance reports as an aid to troubleshooting. To make the time stamps accurate, you must set the date and time of the real-time clock upon system installation.

Once you have set the real-time clock, you need to reset it only if the DataSMART has an extended power loss. The real-time clock operates for two hours, nominally, after power is lost.

CAUTION!
When you change the date or time parameters of the real-time clock, all performance data is cleared from all reports except the VC Utilization Report.

Using the command line

Set the date by using the **SD** command. You must have super-user or configuration privileges. The command syntax is:

SD:*mm***,***dd***,***yy*

mm	Specify the month. You can enter the three-letter abbreviation or the number of the month.
dd	Specify the day of the month. The DataSMART performs a range check on the entered value to see if the day is valid for the given month and year.
yy	Specify the last two digits of the year between 1992 and 2091.

TIP
If you want to track between Daylight Savings Time and Standard Time, you will need to reset the "time" parameter when local time changes.

Set the time by using the **ST** command. You must have super-user or configuration privileges. The command syntax is:

ST:*hh***,***mm*

hh	Specify the hour. The time is specified in "24-hour" format, where 12:00 is noon and 00:00 is midnight. Allowed values are 0 to 23, inclusive.
mm	Specify the minutes. Allowed values are 0 to 59, inclusive.

Using the front panel

To set the date and time from the front panel, use these steps.

1. The SET DATE and SET TIME strings are divided into fields. To select a field to change, push Next or Previous until the field is underlined, then push Select.
2. Push Next or Previous to cycle through the allowed field values.
3. When the value you want is displayed, push Select. The LCD displays CLR PERF DATA? to remind you that changing the date or time clears performance data from the performance reports. Push Select again to change the date or time, or push Escape to abort. If you push Select, PERF DATA CLEARD appears on the screen, indicating that the date or time has been reset and the performance data cleared.
4. Repeat steps 1 through 3 to change each field in the date or time string.

Naming the device

Each DataSMART is assigned a device name that appears in alarm messages, performance reports, and at the top of the Main Menu. You can specify any name up to 15 characters long. Usually the name represents your site or the service you are connected to.

The device name specified here is also the name returned with the MIB II *sysName* object.

The default device name is "PORTLAND, OR."

Using the command line

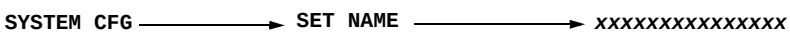
You change the device name by using the **SN** command. You must have super-user or configuration privileges. The command syntax is:

SN:*id*

id	Enter the device name. The name can be up to 15 characters long, including spaces, commas, or colons. A space, comma, or colon may not appear in the first position. Trailing spaces are truncated. Alphabetic characters are saved as upper case.

Using the front panel

A name entered via the front panel can be 15 characters long. To set the name from the front panel, use these steps.



1. When the current device name appears in the display, push Next or Previous to select the character in the field you want to change. When the character field you want to change is underlined, push Select.
2. Push Next or Previous to change the character. When the character you want is displayed, push Select.
3. Repeat steps 1 and 2 until you have changed all the character fields you want.
4. Push Escape. SET NEW STRING? appears in the display. Push Select to confirm or push Escape to abort.

Setting the unit mode

You can configure the DataSMART to operate in Monitor mode or Transparent mode.

Monitor mode gathers Frame Relay statistics and provides all available Frame Relay capabilities, including in-band monitoring and FPINGs. Transparent mode does not allow Frame Relay monitoring, collection of Frame Relay performance statistics, or FPINGs, but is compatible with Frame Relay operations, like any other non-monitoring DSU. Transparent mode is also useful for testing physical functioning of the T1 service.

The default operating mode is Transparent.

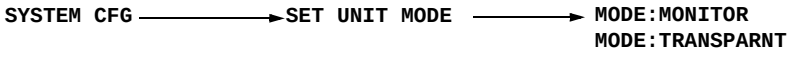
To change between Transparent mode and Monitor mode, use the **SMM** and **SMT** commands. You must have super-user or configuration privileges.

SMM Puts the unit into Monitor mode.

SMT Puts the unit into Transparent mode.

Using the front panel

To set the unit mode:



Enabling/disabling the front panel

To secure the front panel, you need to set a front-panel password, then enable or disable the front-panel pushbuttons as desired. For more information, see "Securing the front panel" on page 29.

Specifying the system clock

The DataSMART times all outputs using one source. For most applications, the DataSMART is set to derive its source clock from the network receive signal (Loop Timing). This is the most common timing setup and should be used if your T1 service provider supplies timing. If your T1 service provider does not supply timing, you must select an alternate source as specified in Table 3.

Figure 4 on page 37 illustrates some common timing applications. When selecting your T1 circuit timing source, it is important to remember this general rule: **There must be only one timing source for the T1 circuit**.

The default is Loop Timing (i.e., the network receive signal).

Table 2—Timing options

Timing option	Description
Loop Timing (**L**)	This option tells the DataSMART to derive its system clock from the incoming signal at the network interface. Select this option if: 1) the T1 service provider is supplying a timing source, or 2) you are using a far-end device in a point-to-point connection as the master timing source.
TI Receive Timing (**T**) (698 only)	This option tells the DataSMART to derive its system clock from the incoming signal at the terminal interface. Select this option if: 1) the T1 service provider is not supplying a timing source, and 2) you want to receive timing from a device beyond the terminal interface, such as a PBX.
Internal Master Timing (uppercase **I**)	This option tells the DataSMART to use its internal oscillator as the system clock. In this case, the DataSMART becomes the master in a point-to-point connection. The far-end device should use Loop Timing. Select this option only if the T1 service provider is not supplying a timing source.

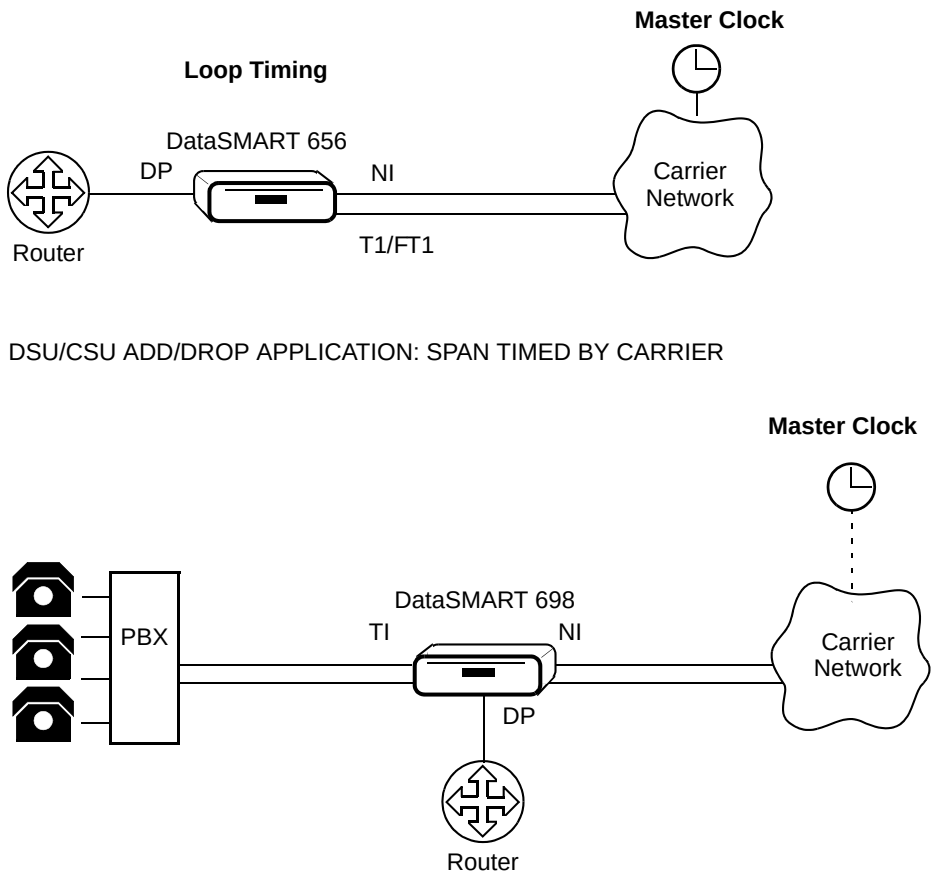
Secondary clock source

If the expected timing source is not present or is lost, the DataSMART defaults to Internal Master Timing. This occurs under the conditions specified in Table 3.

Table 3—Conditions that cause a default to internal timing

Timing option	Condition
Loop Timing	The DataSMART defaults to internal timing if it cannot detect a framed incoming signal at the network interface, either because the signal is lost or because the signal is out of frame or AIS is detected.
TI Receive Timing (add/drop only)	The DataSMART defaults to internal timing if it cannot detect a clock in the incoming signal at the terminal interface, either because the signal is lost or because the signal is out of frame or AIS is detected.

Figure 4—Common timing applications



Setting the clock source using the command line

You set the DataSMART source clock by using the **CLK** command. You must have super-user or configuration privileges. The command syntax is:

CLK:*src*

The *src* value specifies the source clock as:

L	Loop Timing
T	TI Receive Timing
I	Internal Master Timing

Setting the clock source using the front panel

To specify the clock source from the front panel:

SYSTEM CFG → **CLOCK SOURCE** → **CLOCK:INTERNAL**
CLOCK:LOOP
CLOCK:TERMINAL

Setting auto-logout for the control port

You can program the DataSMART to automatically log out a user who has been inactive for a specified period of time. This feature helps prevent situations where:

- A user with a high privilege level forgets to log out, leaving the system open to unauthorized users
- A user forgets to log out and blocks other users from logging in
- A Telnet connection breaks down and hangs the connection

You can specify an auto-logout of 0 (off), or from 1 to 60 minutes, inclusive. A setting of 0 disables the auto-logout timer for users who log in via a serial device connected to the control port. It does not disable the timer for users who login via Telnet—you cannot disable auto-logout for this type of remote login. When the timer is set to 0, the DataSMART defaults to a 15-minute auto-logout period for Telnet.

The default for auto-logout is 0 (off).

Using the command line

To specify an auto-logout period for the control port, use the **ALGOUT** command. When you set the timer to a value greater than 0, that value is used as the auto-logout period for the control port and for Telnet logins.

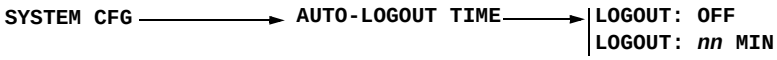
You must have super-user or configuration privileges to use the **ALGOUT** command. The command syntax is:

ALGOUT:*n*

n	Specify the auto-logout period in minutes, from 1 to 60, inclusive. 0 disables the timer (the auto-logout period for Telnet logins becomes 15 minutes).

Using the front panel

To specify an auto-logout for the control port from the front panel:



The allowed values are 1 to 60 minutes, or OFF.

Setting auto-logout for the front panel

The front-panel auto-logout feature prevents you from inadvertently leaving the front panel in an enabled state. See “Securing the front panel” on page 29 for more information.

Zeroing all counters

If you change the configuration parameters for the DataSMART, you may want to clear the performance database. You do this by zeroing all counters. This clears the data from the following:

- User NI Short and Long Performance reports
- User TI Short and Long Performance reports (698 only)
- Far-end PRM Short and Long Performance reports
- User NI Statistical Performance report
- User TI Statistical Performance report (698 only)
- Error threshold counters
- NI/DP Statistical Report
- VC Statistical Report
- VC Utilization Report
- VC Availability Report
- VC Delay Report
- VC Frame Delivered Report

It does not clear the data from:

- Alarm History report
- Security History report

Using the command line

To zero the counters, use the **ZALL** command. You must have super-user or configuration privileges.

Using the front panel

To zero the counters from the front panel:

SYSTEM CFG → **ZERO COUNTERS** → **ZERO COUNTERS ?**

Push Select to zero the counters or Escape to abort. If you push Select, the message PERF DATA CLEARD is displayed, indicating that the counters have been zeroed.

Obtaining new system software

The process for obtaining the latest DataSMART system software has three parts:

- Your company's network administrator or system administrator downloads the file from http://www.kentrox.com/support.
- The administrator then places the file on your company's TFTP host system. (The file must be in the TFTP host's default TFTP directory.) The administrator then informs you of the TFTP host's IP address.

  The TFTP IP address must be in your unit's Source Address Screening list if Source Address Screening is enabled. (See "Setting up IP source address screening" on page 88.)
- Using any active IP connection, you download new system software into the DataSMART unit's flash memory. (See Chapter 6 for information on selecting an IP connection.) After the file is successfully downloaded, enter the **BOOT:I** command to restart the unit and execute the software you just downloaded.

Once you have booted your unit from the updated software, that software version becomes the active software version and is booted when you restart the unit or reset defaults.

You cannot download software or boot the unit from the front panel.

Use the following command to download a software update. You must have super-user privileges.

TSWDL:*i*

i	Enter the IP address of the TFTP host where the software update is stored. Valid addresses are 0.0.0.0 to 255.255.255.255.

Use the following command to boot the unit. You must have super-user privileges.

BOOT	Boots your DataSMART unit from either the active or inactive memory bank.

NOTE

Booting the unit will log out all users, execute the self-test, zero counters in the performance reports and clear the Security History and Alarm History reports, and reset all performance data.

Obtaining product version information

If you call Kentrox Customer Support, you should have the model and serial numbers for your DataSMART available to give to your representative. You can obtain this information from the command line or the front panel.

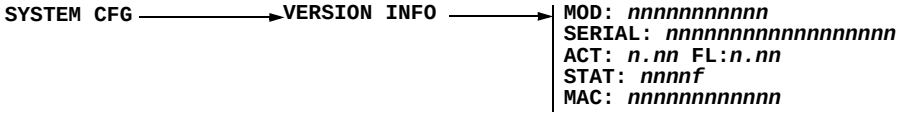
Using the command line

Use the **WYV** command to obtain version information. You need super-user, configuration, or maintenance privileges. The DataSMART displays the version information on the screen, similar to the following.

```
KENTROX      01-72696001, SERIAL nnnnnnnnnnnnnnnnn
STAT 0101F, ACTIVE 1.nn, INACTIVE 1.nn
MAC ADDRESS 008051nnnnnn
```

Using the front panel

To obtain version information from the front panel:



NOTE

Because the display is limited to 16 characters, the 18-character serial number is scrolled left and right to allowing viewing of the full number.

Resetting to default values

You can reset the DataSMART to its default power-up state at any time. The DataSMART will:

- Log out all users
- Restart its control program and execute self test
- Reset all configuration parameters to their default state, including bandwidth assignments and IP addresses
- Zero counters in the performance reports and clear the Security History and Alarm History reports

Once self-test has been completed, you can log into the unit.

CAUTION!
A reset to defaults causes a service disruption until the DataSMART unit is reconfigured for service. (If your required configuration is identical to the default, the service disruption lasts only as long as it takes for the unit to reboot.)

Using the command line

To reset the DataSMART to its default configuration, use the **RSD** command. You must have super-user or configuration privileges.

Using the front panel

To reset defaults from the front panel:

`SYSTEM CFG` → `RESET DEFAULTS` → `RESET DEFAULTS ?`

Push Select to confirm or Escape to abort.

Clearing stored information

The actions that cause the DataSMART to clear its configuration and performance data are summarized in Table 4.

Table 4—Actions that clear stored information from the DataSMART

Action	Clears all configuration data	Clears Alarm History and Security History reports	Clears all other reports
Set date or time (**SD** or **ST**, page 33)	Not cleared	Not cleared	Cleared
Zero all counters (**ZALL**, page 39)	Not cleared	Not cleared	Cleared
Cycle power to unit	Not cleared	Cleared	Cleared
Boot unit (**BOOT**, page 39)	Not cleared	Cleared	Cleared
Reset to defaults (**RSD**, page 41)	Cleared	Cleared	Cleared

Configuring the control port

You need to set up the control port parameters if you plan to communicate with the DataSMART via a DCE control port. These parameters must be set up regardless of whether you plan to communicate through a terminal with an ASCII connection, a modem, or a SLIP connection for Telnet or SNMP.

There are four steps to using a control port:

1. Connect the proper serial cable between the control port and the control device.

   Step 1 is covered thoroughly in the DataSMART 696/698 Installation Guide. This section does not repeat that information.

2. Specify the character protocol of the control device to match the protocol of the DCE control port: 9600 baud, no parity, 8 data bits, and 1 stop bit.

3. Specify whether or not you want characters received at the control port to be echoed back to the control device.

4. Specify your serial IP network protocol (SLIP) if you are using a serial protocol for Telnet or SNMP.

   Step 4 is covered in Chapter 6, under "Selecting an IP network interface" on page 82.

NOTE
When the unit is configured for SLIP, only IP packets are recognized on the control port. Therefore, you should set up your IP configuration as described in Chapter 6 before selecting SLIP.

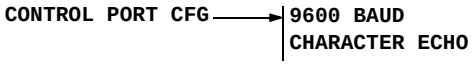
Command-line access

The commands for configuring control ports are listed below (enter **CC** to see this display).

```
                CONTROL PORT CONFIGURATION MENU
EE / DE - Enable/Disable Character Echo
CCV     - View Control Port Configuration
```

Front-panel access

The front-panel commands for configuring the control port are as follows.



Viewing the current configuration

You can look at the current control port settings by executing the **CCV** command. This command displays the View Control Port Configuration screen, as shown below.

TIP
Both input signals must be ON before you can communicate through the selected control port.

```
        VIEW CONTROL PORT CONFIGURATION

Echo      Control Port  CP Setup
--------  ------------  ---------
ENABLED   DCE            96,N,8,1

DCE Inputs
----------
RTS    DTR
---    ---
ON     ON
```

Field	Description
Echo	This field tells you if character echo is enabled or disabled.
CP Setup	This field tells you the protocol settings of the control port: baud rate in hundreds, parity, data-bits-per-character, and stop-bits-per-character.
DCE Inputs	These fields tell you the control port input signal state for RTS and DTR. Possible values for each include ON or OFF.

Configuring the physical connection

The DataSMART is set up with the following character protocol:

baud = 9600
parity = NONE
data bits per character = 8
stop bits per character = 1

If the control device you are using is set differently from the DataSMART, you must change the settings on the control device. You cannot change the protocol settings of the DataSMART.

Enabling/disabling character echo

When character echo is enabled, all printable characters sent to the control port are echoed back to the control device (e.g., characters are echoed on the screen of the control device). If character echo is disabled, characters are not echoed back to the control device.

The default for character echo is “enabled.”

Using the command line

You can use the **EE** and **DE** commands to enable or disable character echo. You must have super-user or configuration privileges.

EE Enable character echo.

DE Disable character echo.

Using the front panel

To enable or disable character echo from the front panel:

CONTROL PORT CFG → **CHARACTER ECHO** → **ENABLE DISABLE**

Connecting control ports to a modem

Connect a modem to the DTE port *after* configuring the modem with the AT commands in the list below. It is essential to configure the modem *before* connecting it to the DTE port because many modems cannot be configured afterwards. This configuration sets auto-answering, flow control, and some other parameters essential to successful communication.

Use only a modem that is compatible with the following AT commands.

Table 5—Standard AT command set

AT command	Action	Modem response
ATS0=1	Auto answer on first ring	OK
AT&K0 SLIP only. Not supported by all modems.	Disable XON/XOFF (Use this command in SLIP mode only.)	OK
AT&C1	DCD is asserted by modem when connection is made	OK
AT&D1	Enter command mode if DTR goes low	OK
Enter the following commands carefully. The characters entered will not be echoed and there will be no responses.		
ATQ1	Modem does not return codes	No response
ATE0	Modem does not echo command characters	No response
AT&W0	Store current configuration as user profile 0	No response
AT&Y0	Specify user profile 0 as power-up configuration	No response

Configuring alarms

Using the commands in the Alarm Configuration menu, you can configure the DataSMART to enable or disable alarm messages, set thresholds and threshold evaluation times, and change the alarm deactivation period.

TIP
If you are using an SNMP network management tool, you can enable or disable four types of SNMP traps (start, link, authentication, and enterprise) independently of whether you enable or disable alarms in ASCII. You will need to make sure your IP network interface is properly configured so that traps are sent to the right destination (see "Selecting an IP network interface" on page 82).

As part of the overall system setup, you can specify the types of alarm messages output by the DataSMART. You can:

- Enable or disable the generation of alarm messages.
- Set the errored second (ES) and unavailable second (UAS) thresholds upon which EER alarms are generated.
- Specify the "sliding" time period for ES or UAS threshold evaluation.
- Specify whether or not an alarm should be generated on an incoming yellow condition.
- Specify the duration of the DataSMART alarm deactivation period.

Alarms are always issued in ASCII format.

This section describes how to set up the configuration parameters for alarms.

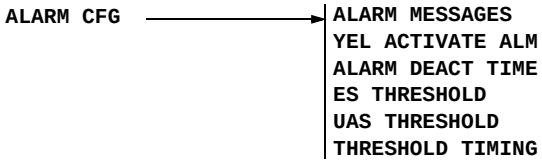
Command-line access

The commands for configuring alarms are listed below (enter **AC** to see this display).

```
                ALARM CONFIGURATION MENU

EAM / DAM       - Enable/Disable Alarm Messages

EYL / DYL       - Enable/Disable YELLOW Activating an Alarm
DACT:<n>        - Alarm Deactivation time in seconds, n = 1..15
EST:<n>         - Errored Second Threshold, n = 0 .. 900
UST:<n>         - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60      - Set Threshold Timing to 15 or 60 Minutes

ACV             - View Alarm Configuration
```

Front-panel access

The front-panel commands for configuring alarms are as follows.



Viewing the current configuration

Before changing the alarm configuration parameters, you may want to look at the current settings. You can do this by executing the **ACV** command. This command displays the View Alarm Configuration screen, as shown below.

```
        VIEW ALARM CONFIGURATION

Message     Alarms Activated  Alarm Deactivation
            LOS+AIS+OOF       Seconds
----------  ----------------  ------------------
DISABLED    +YEL+EER          15

EST  UST  Threshold
          Timing
---  ---  ---------
13   10   15
```

Field	Description
Message	This field tells you if alarm messages are enabled or disabled. Alarm messages are displayed in user (ASCII) format.
Alarms Activated	This field tells you what types of conditions generate alarms. LOS, AIS, and OOF always generate alarms; you can enable or disable alarms for EER and incoming yellow.
Alarm Deactivation Seconds	This field tells you how many seconds the DataSMART continues in an alarm state once the alarm condition has been cleared.
EST, UST	These fields tell you the alarm thresholds for errored second (ES) and unavailable second (UAS), respectively. A zero (0) value means that EER alarms for ES or UAS have been disabled.
Threshold Timing	This field tells you the “sliding” time period the DataSMART uses for ES and UAS threshold evaluation. The period can be either 15 or 60 minutes.

Enabling/disabling alarm messages

The DataSMART outputs an alarm message to your control device when it enters an alarm state. This message identifies the alarm type, the time and date of the alarm occurrence, and the device name and address of the unit sending the message.

You can disable this alarm message output. For example, you may want to do this if you are using a “polling” program to monitor alarms on the devices in your network.

The default for alarm message output is disabled.

NOTE

Disabling alarm messages does not affect the other alarm reporting mechanisms in the DataSMART, including the Alarm History report, the System Status report, SNMP traps, and LED illumination.

Using the command line

To enable or disable alarm messages from the command line, use the **EAM** and **DAM** commands. You need super-user or configuration privileges.

EAM Enable alarm messages.

DAM Disable alarm messages.

Using the front panel

To enable or disable alarm messages from the front panel:

ALARM CFG → **ALARM MESSAGES** → **ENABLE DISABLE**

Enabling/disabling alarms on incoming yellow

The DataSMART generates an alarm message if it detects an incoming yellow alarm code at the network interface, and thus notifies you of a far-end problem. If you do not want this notification, you can deactivate this alarm message. You might also want to deactivate this alarm message if you are using SF framing and are receiving bit patterns that generate a false yellow indication.

The default is to generate an alarm message on incoming yellow (enabled).

Using the command line

To enable or disable activation of an alarm on incoming yellow, use the **EYL** and **DYL** commands. You must have super-user or configuration privileges.

EYL Enable alarm activation on incoming yellow.

DYL Disable alarm activation on incoming yellow.

Using the front panel

To enable or disable alarm activation on an incoming yellow alarm:

ALARM CFG → **YEL ACTIVATE ALM** → **ENABLE DISABLE**

Setting the threshold for errored seconds (ES)

You can specify that the DataSMART generate an EER alarm on excessive errored seconds (ESs). This allows you to monitor the line for errors and detect problems that are not described by signal loss or out-of-frame alarms.

You set up an EER alarm on excessive ESs by using the **EST** command to specify the error threshold. You can specify a threshold value from 0 to 900, inclusive. A value of 0 disables EER alarm activation on errored seconds; a value of 900 means that an alarm will be generated if an ES occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see page 49). The window is a “sliding” window.

The default threshold is 13 errored seconds and the default window is 15 minutes ($\sim 10^{-8}$).

Using the command line

To set the ES threshold, use the **EST** command. You need super-user or configuration privileges. The command syntax is:

EST:*n*

n — Enter the number of ESs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables EER alarm activation on an ES condition.

Using the front panel

To set the ES threshold from the front panel:

The allowed values are 1 to 900, or DISABLE (off).

Setting the threshold for unavailable seconds (UAS)

If your line is experiencing chronically high error rates, you may elect to disable the errored second (ES) threshold and just use the unavailable second (UAS) threshold for generating EER alarms. This decreases the alarm sensitivity significantly, since a UAS occurs at the onset of ten consecutive severely errored seconds (SESs).

You use the **UST** command to specify the threshold used for generating an EER alarm on UASs. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on unavailable seconds; a value of 900 means that an EER alarm will be generated if an unavailable second occurs every second of a 15-minute time window (60 x 15).

You can set the time window to 15 minutes or 60 minutes by using the **ST15** or **ST60** command, respectively (see page 49). The window is a “sliding” window.

The default threshold is 10 unavailable seconds and the default time window is 15 minutes.

Using the command line

To set the UAS threshold, use the **UST** command. You need super-user or configuration privileges. The syntax for the command is:

UST:*n*

n — Enter the number of UASs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables alarm activation on a UAS condition.

Using the front panel

To set the UAS threshold from the front panel:

The allowed values are 1 to 900, or DISABLE (off).

Specifying the error threshold evaluation window

You can a specify a 15-minute or a 60-minute "sliding" time window for error threshold evaluation. If the specified error threshold is exceeded during this sliding window, the DataSMART generates an EER alarm. Use the 15-minute window for increased error sensitivity; use the 60-minute window for a longer term view of line quality.

The following table relates evenly-distributed bit error rates and the number of ESs that will occur in 15- and 60-minute time periods.

Error rate	ESs in 15 minutes	ESs in 60 minutes
1×10^{-6}	900	—
1×10^{-7}	135	540
1×10^{-8}	13	54
1×10^{-9}	1	5

The default window for threshold evaluation is 15 minutes.

Using the command line

To specify the sliding window for threshold evaluation, use the **ST15** and **ST60** commands. You must have super-user or configuration privileges.

ST15 Set the sliding window to 15 minutes.

ST60 Set the sliding window to 60 minutes.

Using the front panel

To set the sliding window from the front panel:

`ALARM CFG` → `THRESHOLD TIMING` → `15 60`

Setting the alarm deactivation time

You can program the DataSMART to remain in an alarm state up to 15 seconds after an alarm condition has cleared. This deactivation period applies to the following alarms:

- NI LOS and TI LOS
- NI AIS and TI AIS
- NI OOF and TI OOF
- NI YEL and TI YEL
- NI EER and TI EER

The default alarm deactivation time is 15 seconds.

Using the command line

To set the alarm deactivation time, use the **DACT** command. You must have super-user or configuration privileges. The command syntax is:

DACT:*n*

n Set the deactivation time from 1 to 15 seconds.

Using the front panel

To set the deactivation time:

ALARM CFG → **ALARM DEACT TIME** → **DACT:** ***nn***

The allowed values are 1 to 15 seconds.

CHAPTER

5 *Configuring interfaces*

This chapter covers the following topics:

- Configuring the network interface
- Configuring the terminal interface (add/drop units only)
- Configuring the data port
- Assigning network interface channels to the data port

Configuring the network interface

Configure the unit's network interface so that it is compatible with the T1 signal from the service provider. A properly-configured network interface supplies the performance reports, remote loopbacks, and alarms.

You must set up the network interface parameters to match the requirements of your service provider. The framing format and line coding for the DataSMART must match the framing format and line coding of your T1 line.

Command-line access

The commands for configuring the network interface parameters are listed below. To view this menu, log into the unit you want to configure, then enter **NC**.

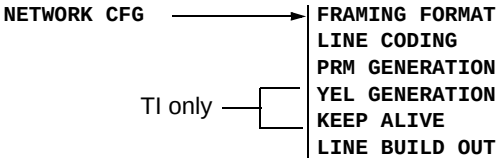
DataSMART 698 only

```
                  NI CONFIGURATION MENU

NSF/NESF/NERC     - NI SF/ESF/Ericsson Framing Format
NAMI / NB8        - NI AMI/B8ZS Line Coding
EPRM / DPRM       - Enable/Disable T1.403 PRM Generation out NI
FKA / UKA         - Framed/Unframed Keep Alive
EYEL / DYEL       - Enable/Disable YELLOW Activation out NI

               Line Build Out
NL0               -  0.0 dB
NL1               -  7.5 dB
NL2               - 15.0 dB

NCV               - View NI Configuration
```

All these commands (except Line Build Out) apply to both the transmit and receive directions on the network interface. There is no way to configure the two directions separately.

Front-panel access

The front-panel commands for configuring the network interface are as follows.



You can use the View Network Configuration display to see the current network interface settings. Enter **NCV** at the command-line prompt.

```
        VIEW NETWORK CONFIGURATION

Framing  Line Code  Line Build Out  PRM Generation  Keep Alive
-------  ---------  --------------  --------------  ----------
ESF      B8ZS       0.0 dB          DISABLED        FRAMED 1íS

YEL Generation
--------------
ENABLED
```

Field	Description
Framing	This displays the current network framing: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line Code	This displays the current line coding: AMI or B8ZS.
Line Build Out	This displays the state of line build-out at the network interface. Possible values are 0.0 dB, 7.5 dB, or 15.0 dB.
PRM Generation	This displays the state of ANSI T1.403 Performance Report Message (PRM) generation: ENABLED or DISABLED.
Keep Alive	This displays the state of the Framed Keep Alive option: FRAMED 1s or AIS. It is valid only for add/drop units with all DS0 channels assigned to the terminal interface.
YEL Generation	This displays the state of yellow alarm generation at the network interface: ENABLED or DISABLED. It is valid only for add/drop units with all DS0 channels assigned to the terminal interface.

Specifying NI framing format

TIP
*The following framing formats and line codes usually go together: super frame and AMI (**NSF** and **NAMI**); extended super frame and B8ZS (**NESF** and **NB8**). However, one does not depend on the other.*

You must set the DataSMART network interface to recognize and transmit data in the same framing format used by the incoming T1 line. Three format choices are available: super frame (SF), extended super frame (ESF), or Ericsson-modified super frame.

Note that if the incoming T1 line is in SF format, you may want to disable the DataSMART from generating alarms upon detection of incoming yellow at the network interface. Sometimes data patterns in SF format generate false yellow. See "Enabling/disabling alarms on incoming yellow" on page 47.

The default framing format is extended super frame (ESF).

Using the command line

Use the following commands to specify framing format. You must have super-user or configuration privileges.

NSF	Super frame
NESF	Extended super frame
NERC	Ericsson-modified super frame

NOTE
Framing format "NERC" is the framing format used by some L. M. Ericsson switches in wireless service.

Using the front panel

To specify framing format from the front panel:

`NETWORK CFG` → `FRAMING FORMAT` → `SF ESF ERIC`

Specifying NI line coding

You must set the DataSMART network interface to the line coding specified by your service provider. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeroes substitution).

The default line coding is B8ZS.

Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

NAMI AMI line coding

NB8 B8ZS line coding

Using the front panel

To specify line coding from the front panel:

NETWORK CFG → **LINE CODING** → **AMI B8ZS**

Enabling/disabling T1.403 loopback and PRM generation

You can enable or disable the DataSMART from sending and receiving ANSI T1.403 performance report messages (PRMs). You should enable T1.403 PRMs if either of the following is true:

- Your carrier requires T1.403 PRMs
- You have a point-to-point application and you want to get far-end performance reports at the near end (FESR/FELR)

When T1.403 mode is enabled, the DataSMART does the following:

- Sends PRMs out the network interface to the far-end device
- Receives PRMs from the far-end device (used to collect data for far-end reports)
- Sets and resets remote loopbacks using T1.403-standard codes

The default state is T1.403 mode disabled.

Using the command line

Use the following commands to enable or disable T1.403 mode. You must have super-user or configuration privileges.

EPRM Enable sending and receiving ANSI T1.403 PRMs and loopback set and reset codes.

DPRM Disable sending PRM messages to the network and disable all other activities defined by the standard.

Using the front panel

To enable or disable T1.403 mode from the front panel:

NETWORK CFG → **PRM GENERATION** → **ENABLE DISABLE**

Enabling/disabling yellow alarm output (add/drop units only)

This command has no effect unless all channels are assigned to the terminal interface.

Yellow alarm output should be enabled only if the terminal equipment connected to the DataSMART is incapable of generating a yellow alarm.

If yellow alarm output is enabled, the DataSMART generates and transmits the yellow alarm code toward the network any time an alarm condition is detected on the network interface. The yellow alarm is transmitted two to three seconds after alarm conditions AIS, OOF or LOS arise.

If the alarm output is disabled, the DataSMART will not generate a yellow alarm code.

The default for alarm generation on incoming yellow is disabled.

Using the command line

Use the following commands to enable or disable yellow alarm generation. You must have super-user or configuration privileges.

EYEL Enable generation of yellow alarm.

DYEL Disable generation of yellow alarm.

Using the front panel

To specify a framed or unframed keep-alive signal from the front panel:

NETWORK CFG → **YEL GENERATION** → **ENABLE DISABLE**

Specify the “keep alive” signal for the network interface (add/drop units only)

This command has no effect unless all channels are assigned to the terminal interface.

If the terminal interface enters an out-of-frame (OOF) condition, the DataSMART keeps the network connection alive by sending the network a framed all-1s signal. This masks the presence of an alarm at the terminal end.

You can program the DataSMART to send the network an AIS alarm (unframed all-1s signal) when the terminal signal is out of frame. This generates an alarm at the far end.

The default “keep-alive” signal is a framed all-1s signal.

Using the command line

Use the **FKA** and **UKA** commands to specify the keep alive signal. You must have super-user or configuration privileges.

FKA Send a framed all-1s signal.

UKA Send AIS (unframed all-1s signal).

Using the front panel

To enable or disable yellow alarm generation from the front panel:

NETWORK CFG → **KEEP ALIVE** → **FRAMD 1S AIS**

Specifying transmit line build out attenuation

Your service provider may ask you to set the DataSMART to attenuate (reduce) the T1 signal at the network interface. Three line attenuation settings are available: 0.0 dB (no attenuation), 7.5 dB, or 15 dB.

The line build-out should always be left at 0.0 dB unless another value is specifically requested. Increased attenuation can interfere with the T1 service.

The default line attenuation is 0.0 db (no attenuation).

Using the command line

Use the following commands to specify line attenuation. You must have super-user or configuration privileges.

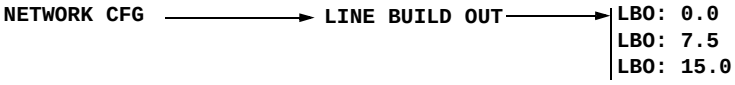
NL0 0.0 dB line attenuation

NL1 7.5 dB line attenuation

NL2 15.0 dB line attenuation

Using the front panel

To specify line attenuation from the front panel:



Configuring the terminal interface (add/drop units only)

Configure the unit's terminal interface so that its framing format, line coding, idle code, and signal equalization are all compatible with your terminal equipment.

You must configure the terminal interface of the DataSMART add/drop unit to make it compatible with the terminal equipment (T1 customer premise equipment) connected to it.

Command-line access

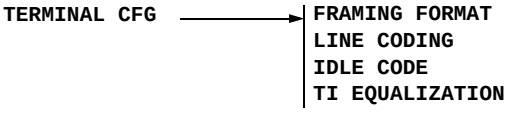
The commands for configuring the terminal interface parameters are listed below (enter **TC** to see this display).

```
                  TI CONFIGURATION MENU

TSF/TESF/TERC  - TI SF/ESF/Ericsson Framing Format
TAMI / TB8     - TI AMI/B8ZS Line Coding
TIDL:<c>       - Idle Code, c = 00-FF Hex

                  TI Equalization
TE0            -   0 - 133 ft
TE1            - 133 - 266 ft
TE2            - 266 - 399 ft
TE3            - 399 - 533 ft
TE4            - 533 - 655 ft

TCV            - View TI Configuration
```

All these commands (except TI Equalization) apply to both the transmit and receive directions on the terminal interface.

Front-panel access

The front-panel commands for configuring the terminal interface are as follows.



Viewing the current TI configuration

Before changing any terminal interface parameters, you may want to look at the current settings. To do this, enter **TCV** at the command-line prompt. This produces a display similar to the one below.

```
       VIEW TERMINAL CONFIGURATION

Framing  Line  Equalization  Idle
Format   Code                Code

-------  ----  ------------  ------
ESF      B8ZS  0..133 ft     7F Hex
```

Field	Description
Framing format	This displays the current framing format applied to the terminal interface: SF (super frame), ESF (extended super frame), or ERICS (Ericsson-modified super frame).
Line code	This displays the current line coding applied to the terminal interface: AMI or B8ZS.

Field	Description
Equalization	This displays the state of signal equalization at the terminal interface: 0-133 ft.,133-266 ft., 266-399 ft., 399-533 ft., or 533-655 ft.
Idle code	This displays the currently-selected idle code. The range is 00 to FF hex.

Specifying TI framing format

TIP
*The following framing formats and line codes often go together: super frame and AMI (**TSF** and **TAMI**); and extended super frame and B8ZS (**TESF** and **TB8**). However, one does not depend on the other.*

You must set the DataSMART terminal interface to recognize and transmit data in the same framing format used by the terminating customer premise equipment, such as a T1 channel bank or digital PBX. You can choose SF (super frame; also known as D4), ESF (extended super frame), or Ericsson-modified super frame.

The default framing format is extended super frame (ESF).

Using the command line

Use the following commands to set the framing format applied at the terminal interface.

TSF Super frame

TESF Extended super frame

TERC Ericsson-modified super frame

NOTE
Framing format "TERC" is the framing format used by some L. M. Ericsson switches in wireless service.

Using the front panel

To specify framing format from the front panel:

`TERMINAL CFG` → `FRAMING FORMAT` → `SF ESF ERIC`

Specifying TI line coding

You must set the DataSMART terminal interface to the same line coding used by the customer premises equipment. Two selections are available: AMI (alternate mark inversion) or B8ZS (binary 8 zeros substitution).

The default line coding is B8ZS.

Using the command line

Use the following commands to specify line coding. You must have super-user or configuration privileges.

TAMI AMI line coding

TB8 B8ZS line coding

Using the front panel

To specify line coding from the front panel:

`TERMINAL CFG` → `LINE CODING` → `AMI B8ZS`

Specifying TI idle code

You can specify the eight-bit idle code that is put into the unused DS0 channels of the terminal interface. The code may have any hex value between 00 and FF.

Whenever an out-of-frame condition occurs at the network interface, the DataSMART DSU puts the idle code into all channels assigned to the terminal interface.

The unit continuously transmits the idle code on any NI channel assigned to "idle."

The default idle code is 7F hex (0111 1111).

Using the command line

Use the **TIDL** command to specify the eight-bit idle code. You must have super-user or configuration privileges. The command syntax is:

TIDL:*c*

c	Enter a hex number with a value between 00 and FF.

Using the front panel

To specify the idle code from the front panel:

TERMINAL CFG → **IDLE CODE** → **IDL COD: *nn* HEX**

Specifying TI signal equalization

If the cable between the DataSMART and the customer premises equipment is longer than 133 feet, you may need to boost the signal level that is output from the terminal interface. By using the **TE***n* commands, you can specify that the terminal interface outputs a DSX-level signal equalized for cable lengths up to 655 feet.

The default equalization setting is 0-133 feet.

Using the command line

Use the following commands to equalize the T1 signal at the terminal interface. You must have super-user or configuration privileges.

TE0	0-133 feet
TE1	133-266 feet
TE2	266-399 feet
TE3	399-533 feet
TE4	533-655 feet

Using the front panel

To specify the signal equalization from the front panel:

TERMINAL CFG → **TI EQUALIZATION** → **TE: 0-133ft**
TE: 133-266ft
TE: 266-399ft
TE: 399-533ft
TE: 533-655ft

Configuring the data port

You can change characteristics of the data port, including timing characteristics and loss-of-signal indicator. Changing these parameters often requires changes at the far end or DTE.

You must configure the data port to match the configuration of the data terminal equipment (DTE) to which it is attached.

Most applications can use the default values. Long DTE cables at high data rates, and perhaps other situations identified by your technical support representative may require changing the settings from their default values.

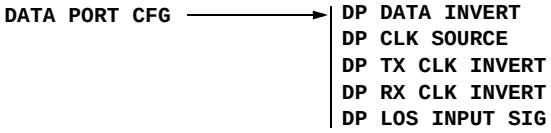
Command-line access

The commands for configuring the data port are listed below. To view this menu, log into the unit you want to configure, then enter **DC**.

```
                DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1

SCLK<n>:<clk>   - Source Clock at Data Port, n=1
                  clk = I (Internal), E (External)
TCLK<n>:<cmd>   - Transmit Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
RCLK<n>:<cmd>   - Receive Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
DPLOS<n>:<los>  - LOS Input Signal at Data Port, n=1
                  los = R (RTS), D (DTR), B (Both), N (No Processing)

DCV             - View Data Port Configuration
```

Front-panel access

The front-panel commands for configuring the data port are as follows.



Viewing the current data port configuration

Before changing any data port parameters, you may want to look at the current settings. To do this, enter **DCV** at the command-line prompt. This produces a display similar to the one shown below.

```
        VIEW DATA PORT CONFIGURATION

                Port 1
                --------
Data Inversion  ENABLED
Source Clock    INTERNAL
Tx Clock Invert DISABLED
Rx Clock Invert DISABLED
LOS Input       RTS
```

Field	Description
Data Inversion	This tells you whether or not data inversion is enabled at the data port. If inversion is enabled, the data is inverted in both directions (i.e., the data from the DTE is inverted before being transmitted to the network, and vice versa).
Source Clock	This tells you which clock signal is being used to clock in transmit data at the data port: INTERNAL or EXTERNAL.
Tx Clock Invert	This tells you whether or not transmit clock inversion is enabled at the data port. If inversion is enabled, transmit data is sampled on the rising edge of the clock signal. If inversion is disabled, transmit data is sampled on the falling edge of the clock signal.
Rx Clock Invert	This tells you whether or not receive clock inversion is enabled. If inversion is enabled, receive data is changed on the falling edge of the clock signal. If inversion is disabled, receive data is changed on the rising edge of the clock signal.
LOS Input	This tells you which signals are currently being used to determine an LOS condition at the data port: RTS, DTR, BOTH, or NONE.

Enabling/disabling data inversion

These commands invert data on the data port. When you enable data inversion, all data received from the DTE is inverted: zeroes are changed to ones and ones are changed to zeroes before being transmitted to the network. Data received from the network is also inverted before being transmitted to the DTE. When data is inverted locally, it must also be inverted at the far-end unit. Data inversion is sometimes used to resolve “ones density” problems caused by a high density of zeroes in the bit stream of the incoming or outgoing data.

The default state is data inversion disabled.

Using the command line

Use the following commands to enable or disable data inversion. You must have super-user or configuration privileges. The command syntax is:

EDI*n* Enable data inversion at data port 1.

DDI*n* Disable data inversion at data port 1.

Using the front panel

To enable or disable data inversion from the front panel, use these steps.

`DATA PORT CFG` → `DP DATA INVERT` → `ENABLE DISABLE`

Specifying data port clocking

You can specify the clock signal used to clock transmit (Tx) data at the data port (see Table 5). Two clock selections are available: internal or external.

Internal clocking means that the transmit data is clocked by the data port's internal clock, which is derived from the DataSMART system source clock.

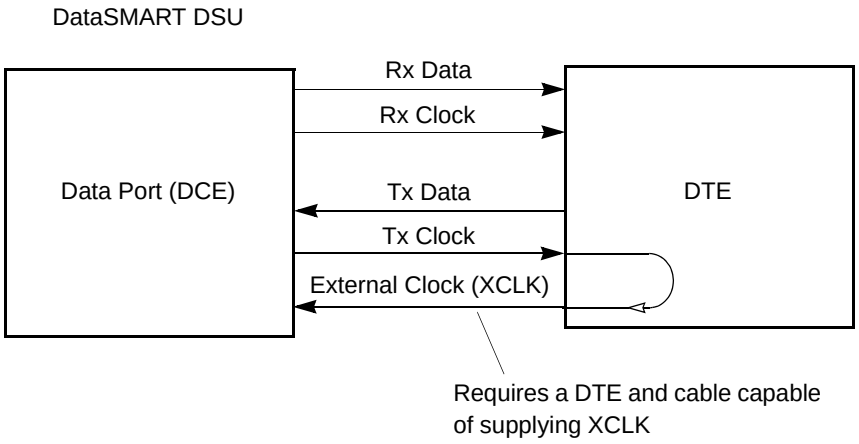
External clocking means that the transmit data is clocked by a signal received on the data port connector's external clock pins (see Table 13 on page 181).

External clocking is typically used:

- With long cables (exceeding 50-100 feet) at high data rates with DTE that supports an external clock signal
- If the DataSMART unit is connected to a Cisco router or to some other DTE with cable that supports the external clock (SCET - DTE source)

The normal operation of synchronous serial data ports provides for three clock signals.

Figure 5—Clock signals at the data port



1. The DCE supplies the receive (Rx) clock signal synchronized with the receive (Rx) data.
2. The DCE also supplies the transmit (Tx) clock signal. The DTE normally transmits its data synchronized to this signal. Most data terminal equipment uses this signal.
3. The external clock signal is the Tx clock signal regenerated by the DTE and synchronized with the DTE's transmitted data. Usually you employ this option when you are receiving excessive data errors at the data port due to propagation delay. Propagation delay becomes a problem when you are using a long data cable (exceeding 50-100 feet) at high data rates. Propagation delay can cause significant phase shift between the Tx clock signal from the DataSMART and the Tx data signal from the DTE.

NOTE

Not all data terminal equipment supports an external clock signal. However, you must have terminal equipment capable of supplying this signal in order to use the external data port clock option.

The default data port clock is internal.

Using the command line

Use the **SCLK** command to specify the data port clock. You must have super-user or configuration privileges. The command syntax is:

SCLK1:*clk*

clk	Enter **E** to specify an external clock source, or enter **I** to specify the internal clock source.

NOTE
***SCLK** specifies data port clocking, not system clocking. System clocking is specified with the **CLK** command.*

Using the front panel

To specify the data port clock from the front panel:

`DATA PORT CFG` → `DP CLK SOURCE` → `INTERN EXTERN`

Enabling/disabling transmit clock inversion

You can invert the transmit (Tx) clock signal and by doing so change the clock edge being used to sample transmit (Tx) data at the data port (refer to Figure 5 on page 62). Transmit data is normally sampled on the falling edge of the transmit clock. If you invert the clock signal, data is sampled on the rising edge of the clock.

The inversion is done on the data port TCLK signal when internal source clocking is chosen and on the XCLK signal when external source clocking is chosen.

Sampling data on the falling edge of the clock is standard; you will seldom need to invert the clock. If the far-end is experiencing data errors, or if the cable connecting the DTE to the data port is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is transmit clock inversion disabled.

Using the command line

Use the **TCLK** command to invert the clock edge. You must have super-user or configuration privileges. The command syntax is:

TCLK1:*cmd*

cmd	Enter **E** to enable clock inversion, or enter **D** to disable clock inversion.

Using the front panel

To enable transmit clock inversion from the front panel:

`DATA PORT CFG` → `DP TX CLK INVERT` → `ENABLE DISABLE`

Enabling/disabling receive clock inversion

You can invert the receive (Rx) clock signal and by doing so change the clock edge being used to clock the receive (Rx) data from the data port to the DTE (refer back to Figure 5 on page 62). Normally, receive data is sampled on the rising edge of the receive clock. If you invert the clock signal, receive data is sampled on the falling edge of the clock.

Sampling receive data on the rising edge of the clock is standard; you will seldom need to invert the clock. If the local DTE is receiving data errors, or if the cable connecting the data port and DTE is long enough to cause undue propagation delays, you may need to invert the clock edge.

The default state is receive clock inversion disabled.

Using the command line

To enable or disable clock inversion, use this command:

RCLK1:*cmd*

cmd	Enter **E** to enable clock inversion, or enter **D** to disable clock inversion.

Using the front panel

To enable receive clock inversion from the front panel:

DATA PORT CFG → **DP RX CLK INVERT** → **ENABLE DISABLE**

Setting up DP LOS (data port loss of signal) processing

You can specify which signals are monitored for LOS at the data port. You can monitor the RTS signal, the DTR signal, both signals, or neither signal.

Data port LOS can be used to identify cases when the DataSMART and network are operating correctly, but the DTE has failed, has lost power, or has been disconnected.

When a data port LOS condition occurs, the DataSMART fills the network interface channels assigned to the data port with the data port idle code (7E hex). DP LOS is reported using the System Status (**S**) command (see "Examining system status" on page 139).

Using the command line

Use the **DPLOS** command to specify the signal(s) monitored for data port LOS. You must have super-user or configuration privileges. The command syntax is:

DPLOS1:*cmd*

cmd is one of the following:

R	Monitor RTS for LOS. This should work correctly with most equipment. Some equipment or cables may need a different setting.
D	Monitor DTR for LOS.
B	Monitor RTS and DTR for LOS. With this setting, the unit detects LOS if both RTS and DTR are low. If either signal is high, LOS is not detected.
N	Disable LOS monitoring (default). The DataSMART ignores RTS and DTR at the data port and assumes that the data port is connected and receiving valid data.

Using the front panel

To specify the signals being monitored for LOS:

DATA PORT CFG → **DP LOS INPUT SIG** → **OFF RTS DTR R+D**

Assigning channels

The T1 line provides access to 24 DS0 channels on the network interface. You can assign some of these channels to the data port, assign others to the terminal interface (add/drop units only), and leave other channels idle. The DataSMART has two tables where you can keep separate configurations to handle differing demands on the T1 line.

Topics in this section

In this section, you'll find the following topics:

- "Planning the channel assignment" before setting up the unit, and why it's important
- "Methods of entering channels"—editing and loading channel configuration tables
- "Assigning network interface channels"—the most commonly-used channel setups
- "Rules for assigning channels", "Assigning channels from the command line", and "Assigning channels from the front panel"—you'll need to read about these topics if you're not using one of the typical channel setups described later in this chapter

Planning the channel assignment

The T1 line has 24 channels you can assign to the terminal interface, data port, or idle.

In some simple cases, you may not need to plan the channel assignment. For example, the default configuration for add/drop units maps each network interface channel to its corresponding channel on the terminal interface. For DSUs without a terminal interface, every network interface channel maps to the data port by default.

NOTE
In more complex cases, it is important to have a channel assignment plan, especially when mapping channels to the data port. The DataSMART Configuration Worksheet in your installation guide can help you assign channels.

The default channel assignments are as follows:

T1 CSU/DSU—all channels are assigned to the data port (24 x 64k=1536 kbps)

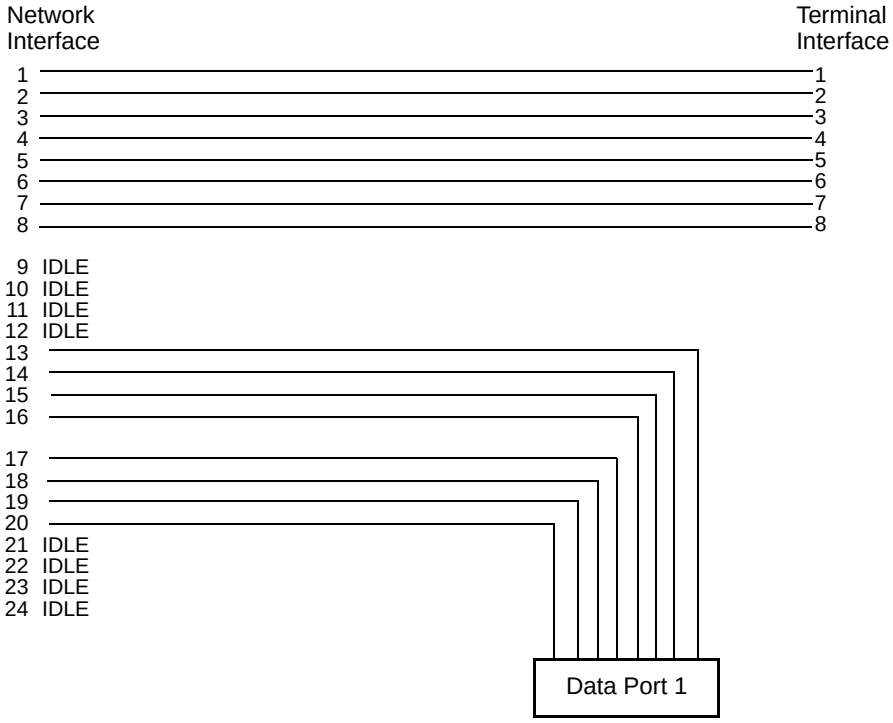
T1 CSU/DSU add/drop—all channels are assigned to terminal interface as voice (TI V)

NOTE

In a point-to-point connection, the units at both ends of the T1 line must have identical channel assignments.

Figure 6 shows a configuration that assigns channels 1-8 to the terminal interface and channels 13-20 to the data port, leaving the remaining channels idle. (This applies to add/drop units only; if your unit is a DSU without a terminal interface, you would leave channels 1-12 and 21-24 idle.) If the data port channels are configured to run at 64 Kbps, the data port speed is 8 x 64 = 512 Kbps.

Figure 6—Sample channel assignment



Methods of entering channels

You can assign channels using the command-line interface or the front-panel interface. There are some fundamental differences between the two methods:

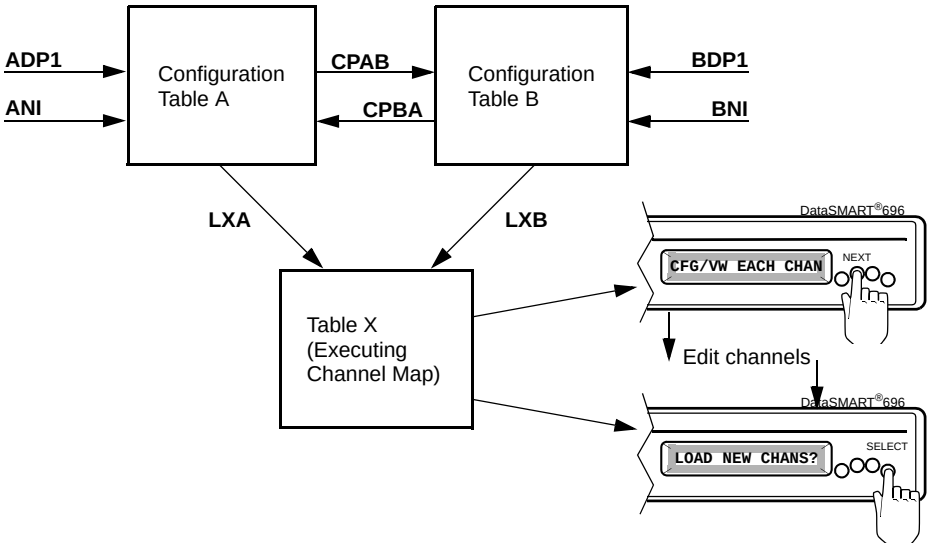
- When you use the front-panel interface, the changes you make are loaded directly into hardware.
- When you use the command-line interface, you are actually editing a table which you then load into hardware in a separate step.

The DataSMART has two tables, A and B, so that you can keep two separate configurations. This feature is useful at sites where, for instance, you have separate configurations for day-time and night-time traffic.

If you assign a channel configuration on the front panel, there is no way to later load it into one of the tables. If you make changes to the configuration using the front panel, it does not affect either of the tables.

Figure 7 illustrates how the configuration table editing commands and front panel editing affect the channel map used by the unit.

Figure 7—Flow chart for editing channel assignments



Editing configuration tables with the command line

The **ADP1** and **ANI** commands edit Configuration Table A.

The **BDP1** and **BNI** commands edit Configuration Table B.

The **CPAB** command copies Table A to Table B, and the **CPBA** command copies Table B to Table A.

Once Table A has been completely edited, the **LXA** command loads it into the executing channel map. The **LXB** command does the same for Table B.

Editing channel assignments with the front panel

For an overview of editing channel assignments with the front panel, see page 75.

Assigning network interface channels

The rest of this chapter contains examples of network interface channel assignments for three typical DataSMART applications, as well as background on setting up a custom channel assignment. Record your application and channel assignment on the DataSMART Configuration Worksheet (found in the Installation Guide). Use the configuration procedure that applies to your application:

- Channels 1-23, CSU using Robbed Bit Signaling; Channel 24, Data Port @ 56 Kbps: see page 69.
- All 24 channels, Data Port @1536 Kbps (24 x 64 Kbps); full rate DSU application: see page 70.
- Fractional T1 DSU @256 Kbps (4 x 64 Kbps): see page 71.
- None of the above: see "Rules for assigning channels" on page 72, "Assigning channels from the command line" on page 73, and "Assigning channels from the front panel" on page 75.

NOTE

When entering commands, be careful to distinguish between uppercase I and numeric 1. To see the syntax for these commands, enter the ***FC*** *command.*

Network management examples are in Chapter 6.

23-channel CSU, Robbed Bit Signaling, 56 Kbps data port (add/drop only)

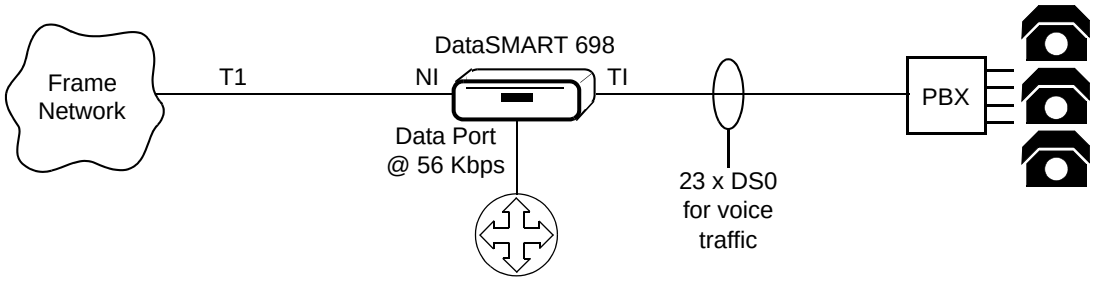
This application sets 23 network interface channels to the terminal interface (voice-type channels) and assigns Channel 24 to the DataSMART data port at 56 Kbps. Use it if your terminal equipment requires the SF or ESF signaling bits.

This application can support in-band management over a Frame Relay permanent virtual circuit (PVC).

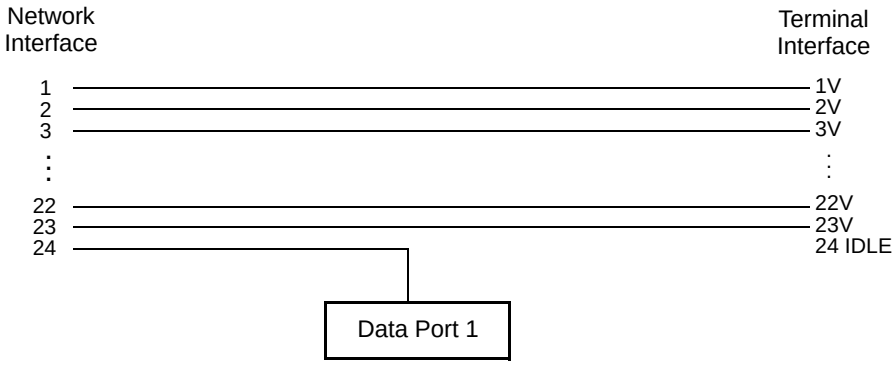
The near-end and far-end DataSMART units must have identical NI channel assignments.

Figure 8—23-channel CSU, Robbed Bit Signaling, 56-Kbps data port

Sample application



Channel map diagram



- The **ANI1-23:V** command assigns network interface channels 1-23 to the terminal interface, voice-type channels.
- The **ADP1:56,24** command assigns network interface channel 24 to the data port at 56 Kbps.

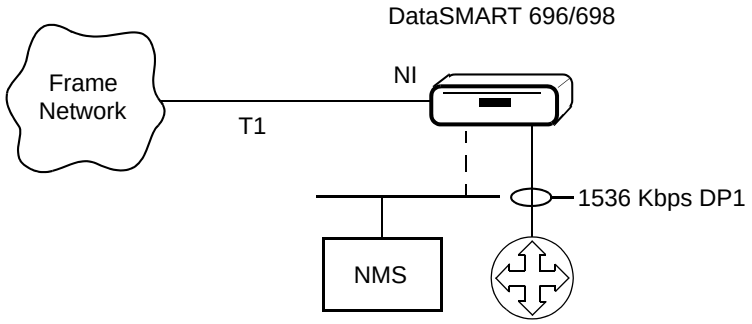
24-channel Full Rate DSU, 1536 Kbps

This application assigns all 24 network interface channels to the data port. All channels are set to 64 Kbps for a total of 1536 Kbps at the data port.

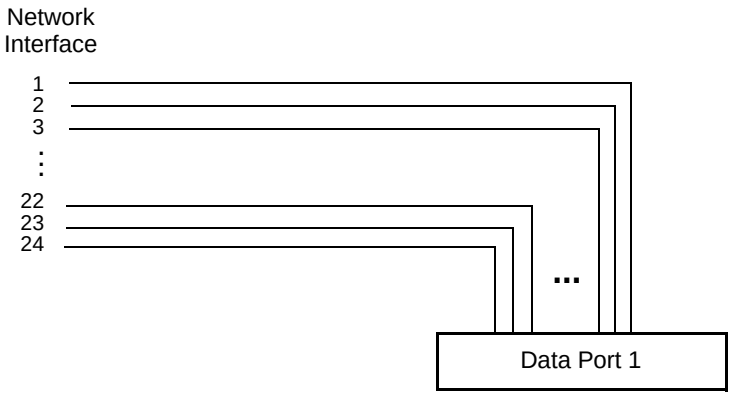
The DataSMART unit can be managed from a local Ethernet port, a local SLIP port, or in-band over the Frame network. See Chapter 8 for details.

Figure 9—24-channel Full Rate DSU, 1536 Kbps

Sample application



Channel map diagram



- The **ADP1:64,1-24** command assigns network interface channels 1-24 to the DataSMART unit's data port at 64 Kbps.

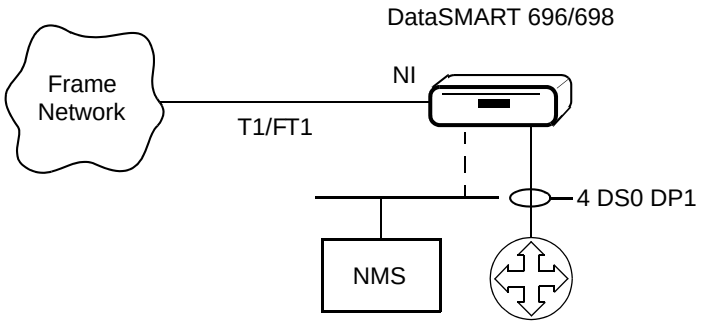
Fractional T1 DSU, 256 Kbps

This application assigns network interface channels 1-4 to the data port. Each data port channel is set to 64 Kbps for a total of 256 Kbps at the data port. All other channels are idle.

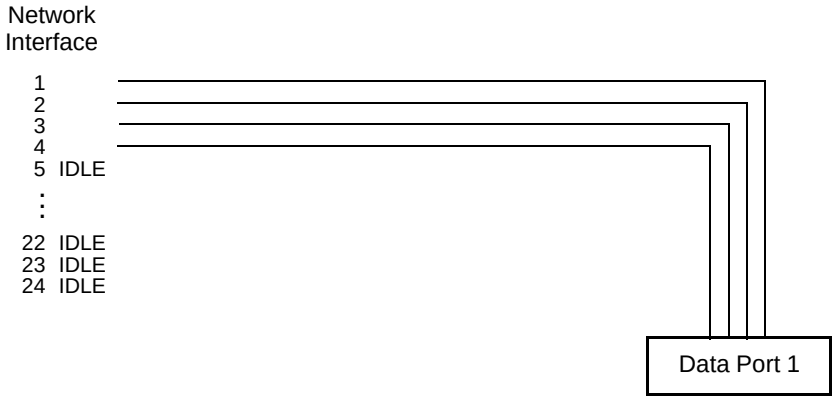
The DataSMART unit can be managed from a local Ethernet port, a local SLIP port, or in-band over the Frame network. See Chapter 8 for details.

Figure 10—Fractional T1 DSU, 256 Kbps

Sample application



Channel map diagram



- The **ADP1:64,1-4** command assigns network interface channels 1-4 to the DataSMART unit's data port at 64 Kbps.
- The **ANI5-24:I** command sets NI channels 5-24 to idle.

NOTE

*To assign more or fewer channels to the data port, modify the above commands. For example, to assign eight channels to the data port, the commands are **ADP1:64,1-8** and **ANI9-24:I**.*

Rules for assigning channels

Rules for assigning data port channels

When assigning network interface channels to the data port and the terminal interface, the channels for the data port must be grouped. Within the group, the channels must be contiguous. For instance, if data port 1 has eight channels to assign, you can assign them in a single group of contiguous channels (1-8), but not two groups of contiguous channels (1-4 and 10-13).

The TI idle code, which goes out the terminal interface on all idle channels, MUST contain sufficient ones to keep the circuit synchronized. When you specify the idle code, make sure you select a code with sufficient ones. (See "Specifying TI idle code" on page 59.)

NOTE

Besides assigning the channels, you must also specify the data rate for the data port. See "Assigning channels to the data port" on page 73.

Rules for assigning terminal interface channels

The rules for channel assignments between the network interface and the terminal interface are:

1. The channel number on the TI side must match the channel number on the NI side.
2. If equipment connected to the TI requires the super frame signaling bits or the extended super frame signaling bits to be passed through the DataSMART DSU (robbed-bit signaling), set the channel type to V (voice).
3. If the equipment connected to the TI requires a 64 Kbps clear channel (no signaling bits), set the channel type to D (data). Use the D option for ISDN PRI service or CCIS-type signaling.
4. You do not need to group the TI channels in any special way, as you do with data port channels.

Compatible and incompatible configurations

The following formats and settings usually go together:

- Super frame, AMI, 56 Kbps channel data rate, one or more channels on the data port
- Extended super frame, B8ZS, 64 Kbps channel data rate, aggregated channels on the data port

The following format-and-setting combination is *not* recommended:

- AMI, 64 Kbps channel data rate (this does not guarantee ones density on the T1 line)

Assigning channels from the command line

You set channel bandwidth using the commands listed in the Fractional T1 Configuration menu. To display this menu, enter **FC**.

```
                FRACTIONAL T1 CONFIGURATION MENU

<table>DP<port>:<rate>[,<nicn>]
                      - DP=Assign NI Channel Map for Data Port
    table A/B         - Tables A or B Containing Channel Assignment
    port  1           - Data Port Number
    rate  56/64       - Channel Rate in 1000 bps
    nicn  1 .. 24     - NI Channel numbers assigned to Data Port or
          1-24        - a contiguous range assigned.

<table>NI<nicn>:<ticn>,<nicn>:<ticn>, ...
                      - NI=Assign NI Channels to TI or IDLE
    table A/B         - Tables A or B Containing Channel Assignment
    nicn  1 .. 24     - NI Channel numbers
    ticn  V,D,I       - Voice/Data on TI Channel or I for Idle

CPAB / CPBA           - Copy A to B or B to A
LXA  / LXB            - Load and Execute Table A or B
TAV  / TBV            - View Table A or B
TXV                   - View Executing Channel Assignment
```

Assigning channels to the data port

This command allows you to edit data port channel assignments and data rates in table A or table B. You must have super-user or configuration privileges to use this command.

NOTE

*Use a numeric **1** (not an uppercase **I**) in the **ADP1** and **BDP1** commands.*

*table***DP1:***rate*[,*nicn*]

table	Specify **A** or **B** to indicate which table you want to edit.
rate	Specify either **56** or **64** Kbps.
nicn	Specify the NI channels that you want to assign to the data port, where *nicn* is one of the following: A single channel number (for example, **11**). A range of channel numbers, delimited by a dash (for example, **2-8**).

Assigning network channels to the terminal interface or IDLE

Use this command to:

- Idle out unused channels on the NI
- Assign network (NI) channels to terminal interface channels (TI) as either “voice” or “data” type (only on add/drop devices).

This command saves the channel assignments into a table (either A or B) which you can later load into the hardware using the **LXA** or **LXB** command.

When you assign an NI channel to the terminal interface, it is assigned “straight across;” the NI channel goes to the TI channel of the same number.

You must have super-user or configuration privileges to use this command. The syntax is:

*table***NI***channels***:D** | **V** | **I**

table	Specify **A** or **B** to indicate which table you want to edit.
channels	Specify the channels in a range of 1 to 24 using one of the following formats: as a single number; as a range of numbers delimited by a dash (for example, 2-12); or as a series of numbers separated by a comma (for example, 2,3,6).
D | **V** | **I**	Specify the characteristic to assign to the channels. You can specify D, V, or I. Specify I if the channel is idle. Specify V (voice) if the channel should be assigned to the TI interface and uses robbed-bit signaling (such as E&M). Specify D (data) if the channel should be assigned to the TI interface and uses common-channeling signal (such as ISDN PRI or D channel).

For example, the following command assigns channels 12 through 20 to the terminal interface using the V characteristic, and puts the information in table A.

ANI12-20:v

Viewing the contents of table A and B

You can inspect the contents of the tables by using the **TAV** and **TBV** commands. You must have super-user or configuration privileges.

TAV	Display the contents of table A.
TBV	Display the contents of table B.

The **TXV** command shows the current assignments. **TXV** does not require any privileges to use.

TXV	Display the current channel assignments on the DataSMART.

To look at table A, for example, enter the **TAV** command from any prompt. The report displays the mapping of NI channels in two different ways. The top of the report lists the ports in the left column and shows rate and all channels assigned to that port to the right. The bottom of the report lists every channel and shows its assignment and whether it is configured for idle or mapped to the data port.

Configuring the interfaces from a table

These commands load a configuration from a table into the hardware, which then operates as configured. You must have super-user or configuration privileges.

LXA	Load configuration from Table A.
LXB	Load configuration from Table B.

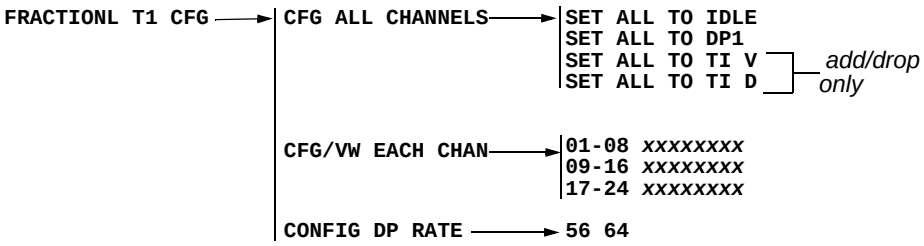
Copying one table into another

You can copy the contents of one table into the other table using the **CPAB** and **CPBA** commands. You must have super-user or configuration privileges.

CPAB	Copy Table A to Table B.
CPBA	Copy Table B to Table A.

Assigning channels from the front panel

The commands available for assigning channels from the front panel are shown below.



Using the CFG ALL CHANNELS command

This command is designed to simplify configuring channels from the front panel. For example, if you plan to configure your unit with most channels going to the terminal interface (voice), you could use SET ALL TO TI V. This assigns every channel to the terminal interface as voice (TI V). Then you could use CFG/VW EACH CHAN to selectively change the other channels.

The steps for setting all channels are:

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Select. SET ALL TO IDLE appears in the display.
5. Push Next or Previous until the desired setting appears in the display, then push Select. “CHANNELS LOADED” appears in the display.

Using the CONFIG DP RATE command

Use this command to configure the data port DS0 channel data rate for the data port.

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Next or Previous until CONFIG DP RATE appears in the display.
5. Push Select. 56 64 appears in the display. The currently-configured value is blinking.
6. Push Next or Previous to change to the desired value, then push Select.

Using the CFG/VW EACH CHAN command

Use this command to assign one channel at a time. You can also use this command to view the current channel assignments from the front panel.

NOTE

The channel configuration display on the LCD is not updated dynamically, If another person is logged into the DataSMART and changes a channel configuration while you are displaying the channel configuration on the LCD, you will not see the changes until the next time you select CFG V/W EACH CHAN.

To view or change the channel assignments, follow these steps.

1. Push Escape until SYSTEM STATUS appears in the display.
2. Push Next or Previous until FRACTIONL T1 CFG appears in the display.
3. Push Select. CFG ALL CHANNELS appears in the display.
4. Push Next or Previous until CFG V/W EACH CHAN appears in the display.
5. Push Select. A display similar to the following appears, with the characters 01-08 blinking:

   ```
   01-08 IIIIIIII
   ```

   The above example shows that channels 01-08 are set to idle. If channels 01-04 were assigned to the data port, the display would show this:

   ```
   01-08 1111IIII
   ```

   The letters that indicate the channel settings can be numeric 1 (for data port 1) or uppercase I (for idle).
6. If you want only to view the channel settings, push Next or Previous to see channels 09-16 and 17-24. If you want to change a channel assignment, go to step 7.
7. To change a channel assignment, push Select. The channel range stops blinking and an underline appears under the first channel letter.
8. Push Next or Previous to move the underline to the position that represents the channel you want to change. For instance, to change channel 2, the display should look like this:

   ```
   01-08 II_IIIII
   ```
9. Push Select. The underline disappears and the letter begins to blink.
10. Push Next or Previous to change the letter to the value you want.
11. Push Select. The letter stops blinking and the underline reappears.
12. Repeat steps 8 through 11 until channels 01-08 are changed to the desired settings.
13. Push Escape. In the display “01-08” will begin to blink. You can now use Next or Previous to switch to ranges 09-16 and 17-24.
14. Push Next or Previous to switch to the other ranges as desired, and repeat steps 7 through 13.
15. When all channels are set as desired, push Escape. A query will ask “LOAD NEW CHANS?” Push Select to load the new channels, or push Escape to exit without making any changes. If you pushed Select, “CHANNELS LOADED” appears in the display.

CHAPTER

6 *Using network management*

The DataSMART DSUs support network management via Telnet and the Simple Network Management Protocol (SNMP).

This chapter tells you how to:

- Configure for Telnet
- Configure for SNMP
- Configure Frame management

About obtaining IP addresses

The procedures in this chapter require a valid IP address. If there is a network administrator or system administrator at your company, he or she is responsible for obtaining valid IP addresses and issuing them to you. All IP-based networks require IP addresses to be unique. Because of this requirement, **you must obtain a valid IP address for your unit to function; your unit's default IP addresses will not work.**

If there is no one at your company who is responsible for obtaining valid IP addresses, contact your Internet service provider. **Kentrox cannot issue IP addresses for you.**

Basic network management (Telnet)

To manage DataSMART with SNMP or Telnet, you must configure the unit to operate with TCP/IP networks. Configuring the unit for management via Telnet is the first step in configuring for SNMP.

The minimal IP network configuration for each unit (enough to enable Telnet and the ping response) consists of:

- Setting the IP interface protocol
- Setting the IP address, netmask, and default router address
- Setting the Telnet password

If you want to use SNMP to manage your DataSMART unit, you must also set the SNMP read, write, and trap community strings.

Command-line access

The DataSMART has two IP management configuration menus:

- The Management Configuration menu contains the commands needed to set up a basic IP network interface and communicate with the unit via Telnet.
- The Advanced Management Configuration menu contains the commands needed to set up SNMP communications with a DataSMART unit.

Super-user or configuration access is required to use either menu.

Enter **MC** to display the Management Configuration menu.

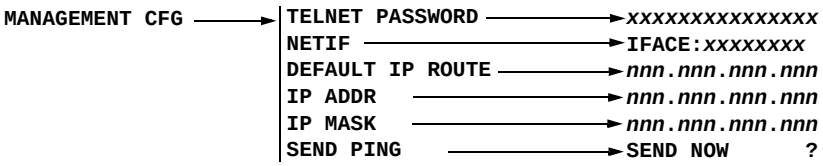
```
                MANAGEMENT CONFIGURATION MENU

TPW:<str>       - Set Telnet Password, str=0 to 15 characters
                  0 characters disables Telnet
NETIF:<p>       - Set IP Network Interface Paths
                  <c>, I = Inband, E = Ethernet, N = None, S = SLIP
SBTP:<m>        - Set BOOTP Mode.  <m> = F (First Start Up),
                  A (All Start Ups), D (Disabled)
IPR:<ipa>       - Set Default Route IP Address (N/A with In-Band)
IPA:<ipa>       - Set IP Addresses
IPM:<mask>      - Set IP Masks
                  <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
ping:[<vc>,<p>,]<ipa>,<n>,<l>
                - Activate PING Test
                  <vc> = 1..1023
                  <p>  = d for data port, n for network (default = n)
                  <ipa>= IP address (xxx.xxx.xxx.xxx)
                  <n>  = number of PINGs to send 1..100
                  <l>  = payload 100..1000 bytes (default = 100)

AMC             - Advanced Management Configuration Menu
MCV             - View Management Configuration
```

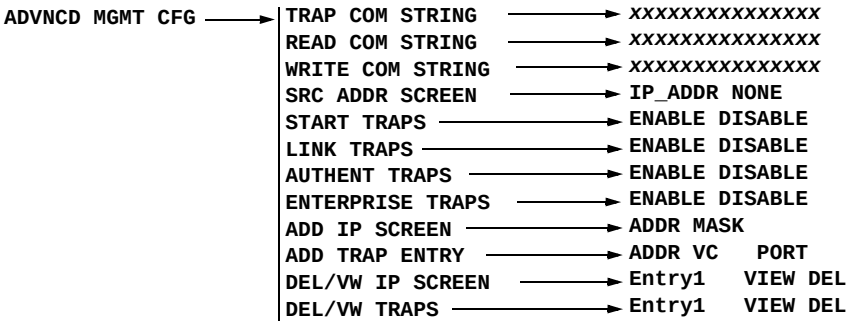
Enter **AMC** to display the Advanced Management Configuration menu.

```
                ADVANCED MANAGEMENT CONFIGURATION MENU

TCS:<str>           - Set SNMP Trap Comm String, str=1 to 15 chars
RCS:<str>           - Set SNMP Read Comm String, str=1 to 15 chars
WCS:<str>           - Set SNMP Write Comm String, str=1 to 15 chars

SSA:<p>             - Set Packet Screening via Source Address
                      p = I (IP Addr), N (None)
TRAP:<c>,<t>-         SNMP Trap Generation c = E (Enable), D (Disable)
                      t = S (Start), L (Link), A (Auth), E (Enterprise)
ADD:T,<ip>[<vc>,<p>]- Add IP Address to Trap Dest List
                      <vc> = Virtual Circuit, <p> = (N)I or (D)ata Port
                      <vc> and <p> are only required for In-Band
ADD:I,<ip>[,mask]   - Add IP Address to Screening List
DEL:<l>,<ip>        - Delete Address from Screening or Trap Dest Lists
                      <l> = I (IP Screen List), T (Trap Dest List)
                      <ip> and [mask] = n.n.n.n, n = 0 .. 255 (dec)
                      [mask] used only for IP Screen List (Optional)

AMCV                - View Advanced Management Configuration
```

Front-panel access

Front-panel access is provided through the MANAGEMENT CFG and ADVNCD MGMT CFG menus.





View the current settings

Before changing any management parameters, you may want to look at the current settings. You do this by executing the **MCV** command. This command displays the View Management Configuration screen. To see the Telnet password, you must have super-user privileges.

```
          VIEW MANAGEMENT CONFIGURATION

Telnet Password  IP Interface Paths       BOOTP
---------------  -----------------------  --------
                 NONE                     DISABLED

IP Addr           IP Mask           IP Default Router
----------------  ----------------  -----------------
192.0.2.1         255.255.255.0     192.0.2.2
```

To see advanced management parameters, enter the **AMCV** command

```
       VIEW ADVANCED MANAGEMENT CONFIGURATION

Trap Comm String   Read Comm String   Write Comm String
-----------------  -----------------  -----------------
snmptrap           public             private

Addr Screening  Traps Enabled
--------------  ----------------------------------
NONE            Start Link Authentication Enterprise

IP Source Address Screening        Trap Destination
---------------------------------  ------------------------
IP Addr           IP Mask          IP Addr
---------------   ---------------  ----------------
192.228.58.1      255.255.255.0    192.228.59.2
192.228.59.2      255.255.255.255  192.228.58.13
```

These IP address values are for illustration only. The source address screening table is empty by default.

Field	Description
Telnet Password	This field tells you the current Telnet password. If there is no Telnet password, the Telnet Server will not be active and you will not be able to Telnet to the unit.
IP Interface Paths	This field tells you the currently-selected IP interfaces. Possible values for this field are ETHER, SLIP, IN-BAND, or NONE.
BOOTP	This field tells you the setting for BootP mode. Possible values are F (first start up), A (all start ups), or D (disabled).
IP Address	This field shows the unit's current IP address.
IP Mask	This field shows the unit's current IP netmask.
IP Default Router	This field tells you the address of the IP default router (does not apply if the IP interface is IN-BAND or NONE).
Trap Comm String	This field tells you the current value of the SNMP Trap Community String. The default value is "snmptrap."
Read Comm String	This field tells you the current value of the SNMP Read Community String. The default value is "public."
Write Comm String	This field tells you the current value of the SNMP Write Community String. The default value is "private."
Addr Screening	This field tells you if the unit is currently screening IP addresses.
Traps Enabled	This field tells you which SNMP trap types will be sent. The trap types are Start, Link, Authentication, Enterprise, or any combination of the above.
IP Source Addr Screening: IP Addr	This field shows which IP addresses are allowed to communicate with the unit. This field can have up to ten entries. Duplicate entries are not valid.
IP Source Addr Screening: IP Mask	This field contains the IP mask that determines which IP subnet the unit belongs to. This field can have up to ten entries. Duplicate entries are not valid.
Trap Destination: IP Addr	This field tells you which IP addresses the unit sends traps to. This field can have up to ten entries. Duplicate entries are valid.

Setting the Telnet password

The DataSMART Telnet server is enabled and disabled via the Telnet password. A null password (i.e. “”, string length of zero) disables Telnet. Any non-null string enables Telnet. The Telnet password can be up to 15 characters long.

To access the unit via Telnet, the Telnet password must be a non-null string and the IP network interface must be enabled and configured properly.

Using the command line

You set the Telnet password using the **TPW** command. The syntax for the command is shown below. You must have super-user privileges.

TPW:*str*

str	Enter the Telnet password. The password can be up to 15 characters long, including spaces. Spaces are not allowed at the beginning of the password, but they are allowed in the middle of the password. Trailing spaces are not truncated.

Using the front panel

The operation of the front panel for this command is different than most other commands. The display is not dynamic. The Telnet password will not be changed until the very end when you confirm the change.

Spaces are allowed at the beginning and in the middle of the password when entered from the front panel.

To set the Telnet password from the front panel:

MANAGEMENT CFG → **TELNET PASSWORD** → ***xxxxxxxxxxxxxxx***

1. Push Next or Previous to move between the fifteen possible characters of the Telnet password. When the character you want is underlined, push Select.
2. Push Next or Previous to increment or decrement the value. When the value of the character field is what you want, push Select.
3. If the entire Telnet password is correct, push Escape. You will be prompted with: SET NEW STRING?. Push Select to set the IP address or push Escape to abort.

Securing your Telnet password

Use the following procedures to prevent your Telnet password from being displayed as it is entered. These procedures also apply when using the DataSMART Installer program.

- To block the display of your Telnet password in the command-line interface, set a super user password through the Management Configuration menu. See “Securing the command-line interface” on page 26.
- To block the display of your Telnet password in the front panel LCD window, set a front panel password, and disable the front panel display. See “Securing the front panel” on page 29.

Once you have completed these steps, your Telnet password will display as five asterisks (*****), no matter how many characters are in the Telnet password.

Choosing an IP network interface protocol

DataSMART 696 and 698 DSUs allow you to choose one or more of the following IP network interface protocols:

- Ethernet
- SLIP over the unit's control port
- In-band via Frame Relay

Each network interface requires you to enter a separate IP address for each unit and an IP netmask.

Table 6—IP network interface options

Option	Command Line	Front Panel	IP Addresses	IP Netmasks	Use this option when...
Ethernet	**E**	ETHERNET	Ethernet	Ethernet	A single DataSMART unit connects to the NMS or router via Ethernet
SLIP	**S**	SLIP	Control Port	Control Port	The DataSMART unit connects to the network host directly using SLIP
In-band	**I**	INBAND	In-band	In-band	The DataSMART is remotely managed in-band via Frame Relay
None	**N**	NONE	N/A	N/A	You are not using SNMP management

The Frame in-band IP network interface

The Frame in-band IP network interface sends IP management data as encapsulated IP messages in Frame format. Depending on the management path, the IP management packets travel from the unit through the network interface over the T1 data stream or through the data port to a router. The unit can receive IP management traffic from either direction.

Selecting an IP network interface

Using the command line

The command syntax is:

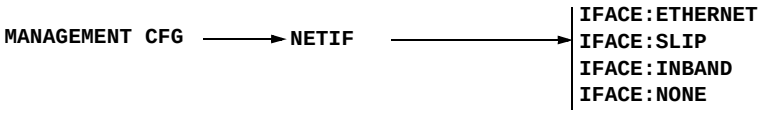
NETIF:*p*

p	Specify the protocol: **E** (Ethernet) **S** (SLIP) **I** (In-band) **N** (none)

The VCT command in the FMC menu specifies if inband management traffic is to be restricted to one virtual circuit (VC).

Using the front panel

To set the IP network interface from the front panel:



When the network interface you want is displayed, blinking with a question mark, push Select, then push Escape, then push Select again.

About IP addressing

To send and receive data across the IP network, every device (or *host*, in IP terminology) on the network requires a unique IP address. An IP address consists of four decimal numbers between 0 and 255, separated by periods. This convention is called *dotted decimal notation*. Each address is composed of two parts: a network part, which identifies the subnet containing the host; and a host part, which identifies the actual host device.

An IP address mask, also called a *netmask*, is used in conjunction with the IP address to determine which part of the address is the network part and which is the host part. In the examples in this guide, the netmask is 255.255.255.0, which sets the first three numbers of the IP address as the network part and the last number as the host part.

Typically, you get IP addresses from your network or system administrator or Internet Service Provider (ISP). If you are the network or system administrator, get a network address from the InterNIC. **Kentrox cannot provide you with IP addresses.** Assign an IP address to each host in the IP network.

Sample configurations with IP addresses

The following examples illustrate different ways of configuring DataSMART units for IP management.

Sample applications

The examples in this section show how to:

- Assign network interface channels on the DataSMART DSU
- Configure the DataSMART network interface
- Assign IP addresses and IP netmasks

Example 1—In-band-managed remote DSU, via Frame

In Example 1, the remote DataSMART unit is set up as a full-rate DSU. The network management system (NMS), located elsewhere in the network, communicates over a permanent virtual circuit (PVC) to the remote site. There are three possible management paths:

- IP management traffic for the DataSMART unit goes through the router, which bounces it back to the DataSMART on the same subnet (see Figure 11).
- IP management traffic for the DataSMART unit shares a PVC with the router, which is on the same subnet (see Figure 12).
- IP management traffic for the DataSMART unit and the router use separate PVCs, and the router and DataSMART are on different subnets (see Figure 13).

Source address screening setup (steps 8 and 9) and SNMP trap setup (steps 10-12) are optional.

Figure 11—Remote DSU managed via Frame in-band, bounce back from router

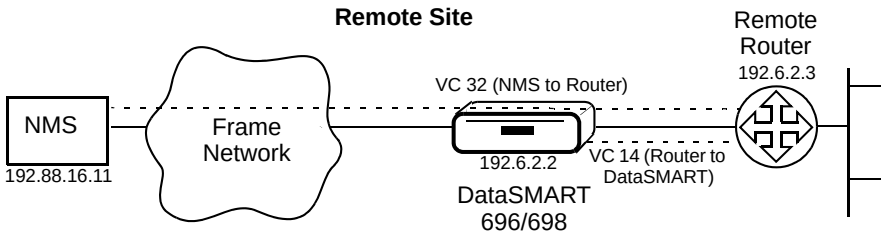


Figure 12—Remote DSU managed via Frame in-band, shared VC between DSU and router

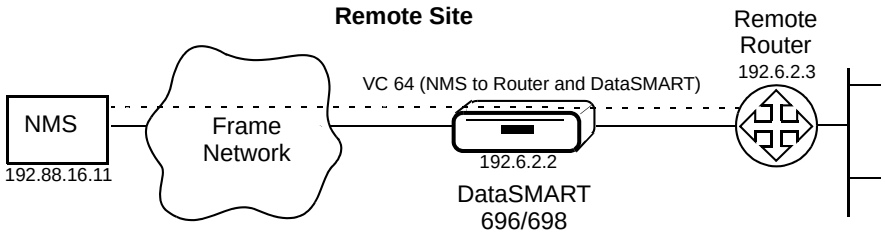
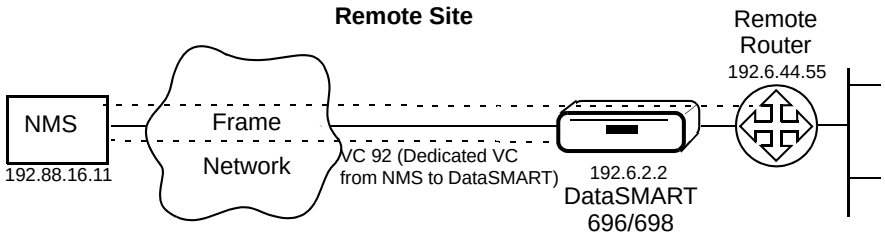


Figure 13—Remote DSU managed via Frame in-band, dedicated VCs for DSU and router



Configuration Commands Use these commands to set up NI channel assignments and IP network management for the DataSMART units shown in all of the examples on page 84:

1. Type **ADP1:64,1-24** to assign all 24 NI channels to the data port at 64 Kbps.
2. Type **LXA** to load network interface configuration Table A into the unit.
3. Type **NETIF:I** to set up a Frame in-band IP management interface.
4. Type **IPA:I, 192.6.2.2** to set the Frame in-band IP address.
5. Type **IPM:I, 255.255.255.0** to set the Frame in-band IP netmask (the default).
6. Type **TPW:KENTROX** to set the Telnet password to KENTROX (all caps).
7. (SNMP trap steps—optional)
   Type one of these commands to send traps to the NMS, depending on the VC configuration the carrier has assigned:
   Bounce-back: Type **ADD:T, 192.6.2.11,14,D** to send traps out the data port.
   Shared VC: Type **ADD:T, 192.6.2.11,64,N** to send traps out the NI.
   Dedicated VC: Type **ADD:T, 192.6.2.11,92,N** to send traps out the NI.

8 (Source address screening steps—optional)
Type **ADD:I, 192.88.16.11** to add the NMS IP address to the source address screening list, ensuring that the NMS can manage the DataSMART.

9 Type **SSA:I** to enable source address screening, ensuring that only the hosts in the source address screening list (i.e., the NMS) can manage the DataSMART.

Setting the IP address

TIP
If you do not know what your IP address and IP netmask should be, ask your network administrator or system administrator. If you do not have a network or system administrator, obtain a set of valid IP addresses from your Internet service provider. ***Kentrox cannot issue IP addresses.***

The IP address is the unique address for a device in the IP network. The default IP address is 192.0.2.1. **You must change this IP address before adding the unit to an IP network.**

Using the command line

You set the IP address by using the **IPA** command. You must have super-user or configuration privileges. The changed IP address takes effect only after you have logged out.

The command syntax is:

IPA:*ipa*

ipa	Enter the IP address using the format *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. An IP address of 0.0.0.0 is not valid.

Using the front panel

The changed IP address takes effect immediately upon pushing Select. To set the IP address from the front panel:

MANAGEMENT CFG → **IP ADDR** → ***nnn.nnn.nnn.nnn***

1 Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.

2 Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.

3 If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

Setting the IP netmask

The DataSMART unit uses the IP netmask to determine if IP traffic is destined for a host on the same IP network as itself. If the traffic is destined for its network, the unit can send it directly to the host. If the IP traffic is destined for a different network, the unit sends it to the IP address of its default router.

The default IP netmask is 255.255.255.0. Changes to the IP netmask take effect upon logout.

Using the command line

You set the IP netmask by using the **IPM** command. You must have super-user or configuration privileges. The command syntax is:

IPM:*mask*

mask	The IP netmask. It takes the form *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. The default is 255.255.255.0.

Using the front panel

To set the IP netmask from the front panel:

`MANAGEMENT CFG` → `IP MASK` → *`nnn.nnn.nnn.nnn`*

1. Push Next or Previous to move between the four fields of the IP netmask. When the field you want has its first character underlined, push Select.
2. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
3. If the entire IP netmask is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP netmask or push Escape to abort.

Selecting the default route IP address

Hosts that are on the same IP network can send IP traffic to each other directly. If a host wants to send IP traffic to a host that is not on the same network, the traffic must be sent to a router that understands the topology of the network. The DataSMART needs to know the address of its default router in order to send packets to another network. This could occur if an SNMP management station is on a different network and is trying to retrieve information from a DataSMART unit.

If a packet is destined for a different network, the unit sends the packet to the IP address of its default router. If there is no default router defined, or if the definition is invalid, the unit discards the packet.

In order for the default router to send a packet to the proper network, you have to configure the default router's static route table. If the default router isn't connected directly to the host, the default router has to link the host address with a forwarding address that will accept the packet and forward it to the host.

NOTE

Do not define a default router if you are using the In-Band IP network interface. Otherwise, you should always set the address of the default router. If a default router does not exist and a DataSMART unit tries to send a packet to a host not on its subnet, the packet will be discarded. This is true for Ethernet and SLIP connections.

The default value for the default router address is 192.0.2.2.

If you are accessing the IP network via Ethernet, the unit's default router must be on the same subnet as its Ethernet IP address.

Using the command line

You must have super-user or configuration privileges. The command syntax is:

IPR:*ipa*

ipa	Enter the IP address using the format *nnn.nnn.nnn.nnn*, where *nnn* can be any number from 0 to 255, inclusive. An IP address of 0.0.0.0 is not valid.

Using the front panel

The changed default IP router address takes effect immediately upon pushing Select. To set the desired IP address from the front panel:

```
MANAGEMENT CFG ──►DEFAULT IP ROUTE──►nnn.nnn.nnn.nnn
```

1. Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select.
2. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
3. If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW ADDRESS?". Push Select to set the IP address or push Escape to abort.

Using PING to test network connectivity

PING sends a signal to a host or gateway, then listens for an echo response. The PING request is sent out the port which is specified by the NETIF command.

The command syntax is:

ping:*vc,p,ipa,n,l*

vc	Specify the virtual circuit. Enter a number between 1 and 1023.
p	Specify *d* to transmit the ping out the data port or *n* to send the PING out the network interface.
ipa	Specify the IP address of the required device.
n	Specify the time between PINGs.
l	Specify the length of the PING payload in octets. Enter a value between 0 and 1000. The default is 100.

To deactivate or exit a PING test, enter Ctrl-C.

Front panel access

To initiate a ping request from the front panel:

```
MANAGEMENT CFG ──►SEND PING ──► SEND NOW       ?──►SEND PING
                                SELECT VC        ──►vc: nnnn
                                SELECT PORT      ──►PORT: NI DP
                                SELECT ADDRESS   ──►000.000.000.000
                                NUMBER OF PINGS  ──►PINGS: nnn
                                LENGTH OF PINGS  ──►OCTETS: nnn
```

Configure your ping request, then push Select to activate the ping. The readouts are updated dynamically as long as the PING is active.

This information is also described in "Setting a PING test" on page 163.

Setting up IP source address screening

DataSMART units can screen IP packets based on the source IP address. This security feature lets you screen out packets from any host that is not supposed to access the unit.

For instance, if you know that only network managers should access the DataSMART, you can add their host addresses to the IP screening list and then lock out all other hosts by enabling IP source address screening.

All source address screening commands (the commands discussed in the rest of this section) are found in the **Advanced Management Configuration (AMC) menu**.

Enabling and disabling IP source address screening

You can enable IP source address screening after filling in the IP addresses allowed access to the DataSMART.

The default is address screening disabled.

Using the command line

You set the IP Source Address Screening using the **SSA** command. You must have super-user or configuration privileges. The command syntax is:

SSA:*c*

The *c* parameter specifies the address screening.

I	Screen based on IP source addresses.
N	No IP address screening.

Using the front panel

To enable or disable IP source address screening from the front panel:

Adding an address or netmask to the IP screening list

Before you can enable IP screening, you must have at least one IP address in the screening list. You can have up to ten addresses total. This list cannot contain multiple entries of the same address, unlike the SNMP trap host list. This list is empty at first power-up.

Adding a netmask to the IP screening list allows you to receive IP packets from any host on the same subnet as the IP address you specify.

Using the command line

You add an IP address to the IP screening list by using the **ADD** command. You must have super-user or configuration privileges. The command syntax is:

ADD:I:*ipa*[,*mask*]

I	Specify IP source address screening.
ipa	Add the specified IP address to the list.
mask	Use this netmask to define the subnet the specified IP address belongs to, and accept IP packets from any host in that subnet. See "Setting the IP address" on page 85 and "Setting the IP netmask" on page 85 for a detailed description of the *ipa* and *mask* fields.

Using the front panel

To add an IP address or netmask to the IP screening list from the front panel:

ADVNCD MGMT CFG → **ADD IP SCREEN** → **ADDR MASK** → ***nnn.nnn.nnn.nnn***

1. Push Next or Previous to move between the four fields of the IP address. When the field you want has its first character underlined, push Select. The field blinks.
2. Push Next or Previous to increment or decrement the value. When the value of the field is what you want, push Select.
3. If the entire IP address is correct, push Escape. You will be prompted with: "SET NEW SCREEN?". Push Select to set the IP address or push Escape to abort.

Viewing and deleting an address from the IP screening list

To delete an address from the IP screening list, source address screening must be disabled. Enabling or disabling source address screening does not take effect until you log out and log back in.

Using the command line

You delete an address from the IP screening list by using the **DEL** command. You must have super-user or configuration privileges. The command syntax is:

DEL:I:*ipa*

I	Specify IP source address screening.
ipa	Delete the specified SNMP manager's IP address from the list. See "Setting the IP address" on page 85 for a detailed description of the *ipa* field.

or

DEL:I:*	Delete all entries in the list by using the * wildcard.

Using the front panel

To view an IP address in the IP screening list or remove the address from the list with the front panel:

ADVNCD MGMT CFG → **DEL/VW IP SCREEN** → **Entry1 VIEW DEL** → ***n*:ADDR MASK** → ***nnn.nnn.nnn.nnn***

1. When DEL/VW IP SCRN appears in the display, push Select; Entry1 VIEW DEL appears in the display.
2. If you want to select a different entry number, push Select. Push Next or Previous until you see the number of the entry you want to view, then push Select.
3. Push Next or Previous until VIEW is highlighted.
4. Push Select. *n*: ADDR MASK appears in the display.
5. Push Next or Previous to switch between ADDR and MASK, then push Select. The IP address appears in the display.
6. Push Select. *n*: ADDR MASK appears in the display.
7. Push Escape. Entry*n* VIEW DEL appears in the display.
8. To delete the entry, push Next or Previous until DEL is highlighted, then push Select. "ADDRESS DELETED" appears in the display.

Configuring for SNMP

To enable the SNMP management capabilities of the DataSMART, the following parameters must be set:

- Set the SNMP community strings, if necessary.
- Add the management hosts to the trap list.

NOTE
This section assumes you have already set up the DataSMART for an IP network. This includes: setting the IP address and netmask and selecting the network interface.

Setting SNMP community strings

There are three SNMP community strings: read, write, and trap. The community strings are another form of (loose) security. If you want to prevent just any SNMP manager from retrieving data from the SNMP agent, you can change the read community string.

Read community string

The read community string controls who can read data from the agent. The default value is “public.”

Write community string

The write community string controls who can write data to the agent using SNMP Sets. The default value is “private.”

Trap community string

The trap community string controls who can read a trap sent from the agent. The default value is “snmptrap.”

Using the command line

You set the SNMP community strings by using the **RCS, WCS,** and **TCS** commands. You must have super-user or configuration privileges. The command syntax is shown below. The strings are allowed to have spaces in them, but you probably won’t want any, as other management stations may not allow spaces in community strings.

RCS:*str*

WCS:*str*

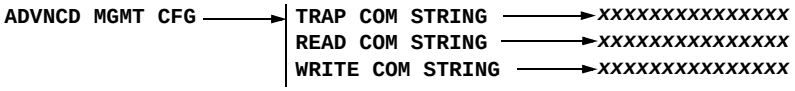
TCS:*str*

where *str* is 1 to 15 characters.

Using the front panel

The operation of the front panel for these commands is different than most other commands. The display is not dynamic. The community string will not be changed until the very end, when you confirm the change.

To set an SNMP community string from the front panel:



1. Push Next or Previous to move between the 15 possible characters of the community string. When the character you want is underlined, push Select.
2. Push Next or Previous to increment or decrement the value of the character you want to change. (The front panel display lets you include any printable ASCII character in a community string.) When the character is what you want, push Select.
3. If the entire community string is correct, push Escape. You will be prompted with, SET NEW STRING?. Push Select to set the community string or push Escape to abort.

Enabling and disabling SNMP traps

DataSMART units can send four kinds of SNMP traps: start, link, authentication, and enterprise. (See "Using SNMP traps" on page 94.) You enable and disable each type of trap separately. All four trap types are enabled by default.

Using the command line

You can not enable or disable more than one trap type with a single command; for example, to enable start and link traps, you must type:

TRAP: E,S
TRAP: E,L

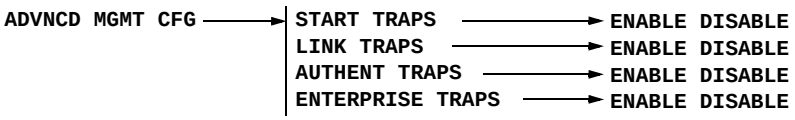
You must have super-user or configuration privileges. The command syntax is:

TRAP:*c,t*

c	Enter **E** to enable the specified traps or **D** to disable them.
t	Specify a trap type to enable or disable: **S** for start, **L** for link, **A** for authentication, and **E** for enterprise.

Using the front panel

To enable or disable SNMP traps from the front panel:



Adding an address to the SNMP trap host list

The SNMP trap host list contains the IP addresses of all IP network hosts that you want the DataSMART unit to send traps to. The SNMP trap host list is empty at first power-up. You add an IP address to the SNMP trap list by using the **ADD** command.

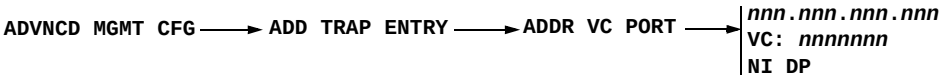
You must have super-user or configuration privileges. The command syntax is:

ADD:T:*ipa*[,*vc*,*p*]

T	Specify SNMP trap list.
ipa	Add the specified IP address to the list. See "Setting the IP address" on page 85 for a description of the *ipa* field.
vc	Specify the virtual circuit on which the trap will be sent out. (Required if **NETIF=I**.)
p	Specify the interface on which the trap will be sent out: **N** for the network interface or **D** for the data port. (Required if **NETIF=I**.)

Using the front panel

To add an IP address to the SNMP trap list from the front panel:



1. To configure ADDR or VC, push Next or Previous to increment or decrement the value, then push Select.
2. To configure PORT, push Next or Previous to toggle between NI and DP, then push Select.

Viewing and deleting an address from the SNMP trap list

If there are multiple entries of a single address in the table, each entry must be deleted. One deletion does not clear out all occurrences of that address.

Using the command line

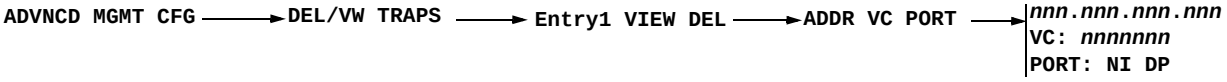
You delete an address from the SNMP trap list by using the **DEL** command. The syntax for the command is shown below. You must have super-user or configuration privileges.

DEL:T:*ipa*

T	Specify SNMP trap list.
ipa	Delete the specified SNMP manager's IP address from the list. See "Setting the IP address" on page 85 for a detailed description of the *ipa* field.
or	
DEL:T:*	Delete all entries in the list by using the * wildcard character.

Using the front panel

To view or delete an IP address from the SNMP trap list:



1. When DEL/VW TRAPS appears in the display, push Select; Entry1 VIEW DEL appears in the display.
2. If you want to select a different entry number, push Select. The entry number is then underlined. Push Next or Previous until you see the number of the entry you want to view, then push Select.
3. Push Next or Previous until VIEW is highlighted.
4. Push Select. *n*: ADDR VC PORT appears in the display.
5. Push Next or Previous to switch between ADDR, VC, and PORT, depending on what you want to view. Then push Select. The item you selected appears in the display.
6. Push Select. *n*: VC PORT appears in the display.
7. Push Escape. Entry*n* VIEW DEL appears in the display.
8. To delete the entry, push Next or Previous until DEL is highlighted, then push Select. “ADDRESS DELETED” appears in the display.

Using SNMP traps

SNMP traps are like DataSMART alarm messages: they indicate alarm conditions in the network.

Configuration for SNMP traps

To use SNMP traps, you must:

- Connect the DataSMART to a TCP/IP network, either in-band, over Ethernet, or over a SLIP connection on the control port.
- Enable any combination of start, link, authentication, and enterprise-specific traps.

SNMP traps also need a destination IP address. You have ten possible trap destinations defined by the trap host list (see "Configuring for SNMP" on page 90). At the trap host destination there must be an SNMP network management application.

Types of SNMP traps

DataSMART units can generate these trap types:

Start traps

- Cold-start

Link traps

- Link-down
- Link-up

Authentication traps

- Telnet Password
- SNMP Rd CommString
- SNMP Wr CommString
- IP Screen

Enterprise traps:

- Excessive Error Rate (EER)

Cold-start trap

The cold-start trap is generated every time the DataSMART is power-cycled. Cold-start traps are not generated until ten seconds after the unit is power-cycled. This allows time for the hardware providing the low-level IP network interface to start up and stabilize before attempting to send a packet.

Link-down trap

A link-down trap is generated when *ifOperStatus* (MIB II) changes to *down*.

Link-up trap

A link-up trap is generated when *ifOperStatus* (MIB II) changes to *up*.

Telnet Password

A Telnet Password trap is generated when an incorrect Telnet password has been entered.

SNMP Rd CommString

An SNMP Rd CommString trap is generated when the DataSMART receives a GET with an incorrect SNMP community string.

SNMP Wr CommString

An SNMP Wr CommString trap is generated when the DataSMART receives a SET with an incorrect SNMP community string.

IP Screen

An IP Screen trap is generated when the DataSMART has received a trap or message from a device whose IP address is not on the Source Screening Address list.

NOTE
The events that generate the Telnet Password, SNMP Rd CommString, SNMP Wr CommString, and IP Screen traps are also logged in the Security History report (see "Interpreting the Security History Report" on page 119). These events are logged into the SHR only once per hour to prevent filling up the report with duplicate entries.

Excessive Error Rate

An Excessive Error Rate trap is generated whenever the Excessive Error Rate threshold is exceeded (see "Specifying the error threshold evaluation window" on page 49).

MIB objects included in SNMP traps

SNMP allows any MIB object to be included in a trap. The DataSMART includes information on its status and that of the T1 line, to speed analysis. Each trap type includes different information.

Cold-start trap

A cold-start trap includes the *ifDescr* and *ifIndex* of all interfaces on the unit.

Link-down trap for a T1 interface

A link-down trap for a T1 interface includes the following:

- ifDescr—"T1 Network Interface"
- ifIndex—this is the instance number for that interface
- dsx1LineStatus—a bitmap of the T1 line's current state
- dsx1CurrentESs—the number of errored seconds for the current interval
- dsx1CurrentUASs—the number of unavailable seconds for the current interval

Link-up trap for a T1 interface

A link-up trap for a T1 interface includes the following:

- ifDescr—"T1 Network Interface"
- ifIndex—this is the instance number for that interface
- dsx1LineStatus—a bitmap of the T1 line's current state
- dsx1CurrentESs—the number of errored seconds for the current interval
- *dsx1CurrentUASs*—the number of unavailable seconds for the current interval

Telnet Password authentication trap

The Telnet Password trap includes the following:

- dsRpShrDateTime—the date and time the event occurred
- dsRpShrEventType—"rpShrTelnetPassword" (Type 1)
- *dsRpShrComments*—the source IP address of the unit that sent the incorrect Telnet password

SNMP IP Screen authentication trap

The SNMP IP Screen trap includes the following:

- dsRpShrDateTime—the date and time the event occurred
- dsRpShrEventType—"rpShrSrcIpAddressScreen" (Type 2)
- *dsRpShrComments*—the source IP address of the device that sent the message to the DataSMART unit

SNMP Rd CommString authentication trap

The SNMP Rd CommString trap includes the following:

- dsRpShrDateTime—the date and time the event occurred
- dsRpShrEventType—"rpShrReadCommString" (Type 3)
- dsRpShrComments—the source IP address of the unit that caused the event

SNMP Wr CommString authentication trap

The SNMP Wr CommString trap includes the following:

- dsRpShrDateTime—the date and time the event occurred
- dsRpShrEventType—"rpShrWriteCommString" (Type 4)
- dsRpShrComments—the source IP address of the unit that caused the event

Traps and alarm conditions

The following table correlates alarm conditions to traps.

Alarm Condition	Trap
NI LOS	Link down on network interface
NI OOF	Link down on network interface
NI AIS	Link down on network interface
NI YEL	Link down on network interface
NI EER	EER enterprise trap on network interface
TI LOS	Link down on terminal interface
TI OOF	Link down on terminal interface
TI AIS	Link down on terminal interface
TI YEL	Link down on terminal interface
TI EER	EER enterprise trap on terminal interface
DP LOS	Link down on data port
Power-up	Cold-start trap

C H A P T E R

7 *Configuring for Frame management*

The DataSMART FrameVision DSUs also support network management via IP connectivity with another Frame Monitoring DataSMART unit over a virtual circuit on a frame network.

This chapter tells you how to:

- Configure Frame management
- Set up Frame Relay Link Managment spoofing
- Monitor the link using FPINGs

Frame management configuration

To establish IP connectivity with another Frame Monitoring DataSMART unit over a virtual circuit on a frame network, you must configure the unit.

The Frame Management Configuration menu lets you do the following:

- FRLM spoofing
- Manage the monitoring table for virtual circuits
- Establish automatic FPING monitoring of all virtual circuits you wish to monitor

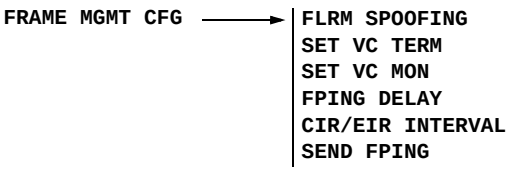
Command-line access

Enter **FMC** to display the Frame Management Configuration menu.

```
                FRAME MANAGEMENT CONFIGURATION MENU

ESP/DSP             - Enable/Disable FRLM Spoofing
VCT:<vc>,<d>        - VC Termination
                      <vc> = 1..1023
                      <d>  = N(NI), D(DP), E(Either)
VCMOD:<vc>,<c>,<e> - Modify VC Monitoring Table
                      <vc> = 1..1023
                      <c>  = CIR 0..1536000 bits/sec
                      <e>  = EIR 0..1536000 bits/sec
FPTIM:<t>           - Set delay between Auto FPINGs
                      <t>  = 5...60 minutes
CIRTM:<t>           - Set time interval for CIR/EIR calculation
                      <t>  = 1...60 sec
FPTST:<vc>[,<p>[,<l>[,<t>]]]
                    - Activate FPING Test
                      <vc> = 1..1023
                      <p>  = D (Data Port), N (Network) (default = N)
                      <l>  = Payload 100..1400 bytes (default = 128)
                      <t>  = FPING frequency 5..255 secs (default = 5)
FMCV                - View Frame Configuration
```

Front-panel access

Front-panel access is provided through the FRAME MGMT CFG menu.



View the current settings

Before changing any frame management parameters, you may want to look at the current settings. You do this by executing the **FMCV** command. This command displays the View Frame Management Configuration screen.

```
        VIEW FRAME MANAGEMENT CONFIGURATION

Frame Type      SPOOFING  TERM VC  TERM DIR  CIR Interval  FPING Delay
--------------  --------  -------  --------  ------------  -----------
FR NLPID        ENABLED   100      DP        21 sec        15 min

                                  Monitored-VC List
 VC    CIR     EIR       VC    CIR     EIR       VC    CIR     EIR
----  ------  ------     ----  ------  ------     ----  ------  ------
11    0K      56K       12    0K      56K       22    0K      56K
23    0K      56K       25    0K      56K       26    0K      56K
27    0K      56K       100   0K      56K
```

Field	Description
FRAME TYPE	This field tells you the encapsulation type monitored on IP management frames. Possible values FR NLPID, and FR ETHERTYPE.
SPOOFING	This field tells you whether or not FRLM spoofing is enabled.
TERM VC	If TERM DIR is set to NI or DP, this field shows which VC is used for VC termination. If TERM DIR is set to Off, this value is inactive.
TERM DIR	This field shows which port receives in-band IP traffic when a specific VC is allocated for IP traffic. Possible values are NI, DP, or Either.
CIR Interval	This field displays the time interval for CIR/EIR calculation.
FPING Delay	This field displays the time delay between auto FPINGs.
VC	This field is the virtual circuit ID. Possible values are from 1 to 1023.
CIR	This field shows the committed information rate (CIR).
EIR	This field shows the excess information rate (EIR).

Using Frame Relay Link Management

Frame Relay Link Management (FRLM) monitors traffic between the Frame Relay switch and the router to determine the status of the Virtual Circuits.

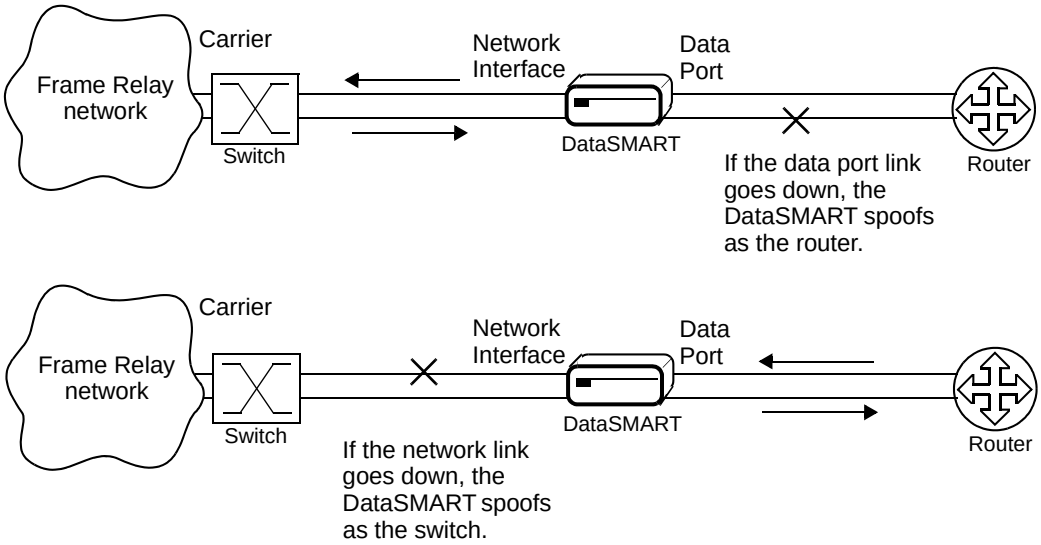
The VCT command allows you to select on which VC to "terminate" in-band IP traffic, and on which interface traffic will be accepted. This setting affects the Full Status message from the switch:

- If VC termination is set for "N", initiating IP traffic between the switch and the DSU, the DSU will ***strip out*** the terminated VC from the Full Status message before retransmitting it out the Data Port. This prevents the router from knowing about this VC.
- If VC Termination is set for "D", initiating IP traffic between the router and the DSU, the DSU will ***add*** the terminated VC to the Full Status message before retransmitting it out the Data Port. This will let the router know that this VC is being used, and is active.

With spoofing enabled, the DataSMART will send a message reporting the status of the VC as well as the physical links. The status for each VC is reported as Active, Inactive, New, or Deleted.

- When the data port link goes down, the DataSMART acts as the router and spoofs messages back to the switch that indicate its link is still alive.
- When the network interface link goes down, DataSMART acts as the switch and spoofs messages back to the router that indicate its link is still alive.

  When spoofing as the carrier service (the DataSMART simulates the switch by sending Status messages to the router) and the VC terminates at the data port, the DataSMART will send out Full Status messages with all VCs set to "inactive" except the terminated VC. This VC will be set to "active" to let the router know that it can still access the DataSMART through in-band IP.



Enabling/disabling FRLM spoofing

This command works in conjunction with the VCT command described below.

Using the command line

You enable and disable spoofing by using the **ESP** and **DSP** commands, respectively. You must have super-user or configuration privileges.

ESP Enable FRLM spoofing.

DSP Disable FRLM spoofing.

Using the front panel

To enable or disable FRLM spoofing operation from the front panel:

FRAME MGMT CFG → **FLRM SPOOFING** → **ENABLE DISABLE**

Selecting the port for VC termination

VC termination lets you select which port receives in-band IP traffic when a specific VC is allocated for IP traffic.

Using the command line

You set VC termination by using the **VCT** command. You must have super-user or configuration privileges.

VCT:<vc>, <d>

vc Enter a virtual circuit ID from 1 to 1023. You can add a VC to the list or edit an existing VC.

d Specify **N** for network interface, **D** for Data Port, or **E** for Either (default).

Using the front panel

To set VC termination from the front panel:

FRAME MGMT CFG → **SET VC TERM** → **SELECT VC:*nnnnnnn***
SELECT DIR: → **EITHER** / **DP** / **NI**

Setting the CIR and EIR for a VC

With DataSMART Frame Monitoring DSU/CSUs, you can determine when you are purchasing too much or too little bandwidth. DataSMART Frame Monitoring DSU/CSUs measure circuit usage and saturation in real time, so you can monitor utilization problems on each virtual circuit. These accurate measurements mean you can purchase only the circuit capacity you need for your particular applications.

The committed information rate (CIR) you purchase from your carrier gives you the guarantee that the Frame Relay network will transport data submitted at or below that rate without loss. If you are regularly transmitting below the CIR, you may be wasting bandwidth and paying too much money. Alternatively, if you are regularly transmitting above the CIR, your network's performance may suffer, because data submitted above the CIR is eligible for discard. This can cause poor performance as routers have to retransmit the discarded data.

The excess information rate (EIR) is a rate over and above the CIR. If the customer sends bursts of data in excess of the CIR, the service provider agrees to accept that data and to make its "best effort" to forward the data.

However, if the burst exceeds the sum of the CIR and the EIR, the service provider may unconditionally discard any data in the burst. Critical traffic over a given VC should rarely, if ever, exceed the sum of CIR and EIR, and never during the network's peak traffic hours.

The sum of the EIR and CIR cannot exceed the access rate.

Using the command line

You modify the CIR and EIR by using the **VCMOD** command. You must have super-user or configuration privileges. The command syntax is:

VCMOD:<vc>, <c>, <e>

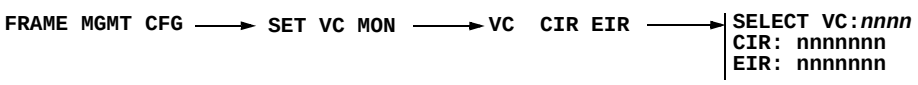
vc	Enter a virtual circuit ID from 1 to 1023.
c	Enter a CIR (in bits per second) from 0 to 1536000. The default is 0.
e	Enter an EIR (in bits per second) from 0 to 1536000. The default is 1536000.

The committed information rate (CIR) and excess information rate (EIR) are determined when you purchase the Frame Relay service.

You need to set the CIR and EIR for each VC being monitored in the VC Utilization Report for the report to provide useful information.

Using the front panel

To modify the CIR and EIR from the front panel:

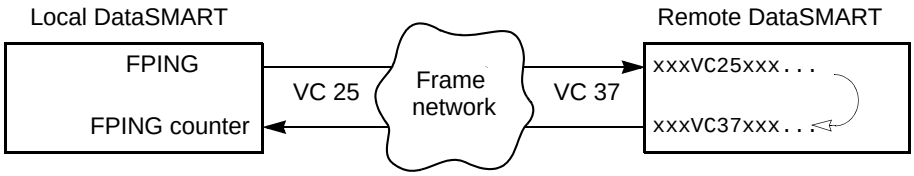


About automatic Frame PINGs

Frame PINGs (FPINGs) provide a way for a Frame Monitoring DataSMART unit to test the integrity and response time of up to 64 virtual circuits (VCs) carrying traffic through the unit. It is designed to make the most accurate available measurement of end-to-end frame network delay.

How FPINGs work

When frame traffic is relatively idle, the local DataSMART unit sends an FPING message to a remote unit over the VC on the frame network. (FPING generation doesn't interfere with data transmission.) The FPING message includes a time stamp and the number of the VC. The FPING message is encapsulated as a frame packet so it can be routed through the frame network. The remote unit receives the FPING message. It replaces the VC number with the one it uses to connect to the local unit, adds its active IP address to the FPING message, and sends it back to the local unit. The local unit receives the echoed FPING message.



As soon as the FPING is received, the local unit calculates the FPING message's round-trip time in milliseconds and updates its performance data. If the FPING round-trip time exceeds a specified threshold, it is considered lost.

How the DataSMART handles automatic FPINGs

The DataSMART can automatically monitor network delay of up to 64 VCs at a time. When it monitors a VC, it sends three FPING messages to the remote unit and compares the time to the threshold time to determine if the round-trip time for that VC exceeds the threshold.

You can also start FPING tests manually, which is useful for testing new or potentially troublesome VCs (see "Troubleshooting connection problems" on page 164). The manual FPING test does not interfere with automatic FPING generation.

Setting the delay between automatic FPINGs

You can define the length of time between automatic FPINGs.

Using the command line

You set the delay between automatic FPINGs by using the **FPTIM** command. You must have super-user or configuration privileges. The command syntax is:

FPTIM:*t*

t	Specify the delay period in minutes, from 5 to 60, inclusive. The default is 15 minutes.

Using the front panel

To set delay between Auto FPINGs from the front panel:

FRAME MGMT CFG → **FPING DELAY** → **DELAY:** ***nnnnnnn***

Setting the interval for CIR/EIR calculation

This command defines the interval for calculating the throughput rates for CIR and EIR threshold comparisons.

Using the command line

You specify the time interval allowed for CIR/EIR calculation by using the **CIRTM** command. You must have super-user or configuration privileges. The command syntax is:

CIRTM:*t*

t	Specify the calculation interval in seconds, from 1 to 30, inclusive.

The default is 10 seconds.

Using the front panel

To set the interval used for CIR/EIR calculation, from the front panel:

FRAME MGMT CFG → **CIR/EIR INTERVAL** → **INTERVAL:** ***nnnnnnn***

Setting an FPING test

You use the **FPTST** command to set up a Frame PING test. You must have super-user, configuration, or maintenance privileges.

The command syntax is:

FPTST:*vc*,*p*,*l*,*t*

vc	Specify the virtual circuit. Enter a number between 0 and 8388607.
p	Specify **D** for data port or **N** for network interface.
l	Specify the length of the FPING payload in octets. Enter a value between 0 and 1400. The default is 32.
t	Specify the time between FPINGs.

To deactivate or exit an FPING test, enter Ctrl-C.

Using the front-panel

To set up a Frame PING test from the front panel:

FRAME MGMT CFG → **SEND FPING** →
- **START FPTEST** → **STARTING FPINGS**
- **SELECT VC** → **VC:** ***nnnn***
- **SELECT PORT** → **PORT: NI DP**
- **SELECT FREQ** → **FREQUENCY:** ***nnnn***
- **SELECT LENGTH** → **LENGTH:** ***nnnn***

For more information on FPING tests, see "Troubleshooting connection problems" on page 164.

CHAPTER

8 Performance monitoring

This chapter describes how the DataSMART unit's performance monitoring facilities help troubleshoot network problems. The DataSMART provides statistical reports and detailed performance reports at both the physical (T1/FT1) level and the transport (Frame) level. It also provides history reports for alarms and security violations.

Report types and their common uses

Report type	Report	Description
T1 performance reports	User NI Performance Reports (**UNSR/UNLR**). See page 108.	Identify T1 receive-line quality problems over a longer time frame than the NSR.
	User TI Performance Reports (**UTSR/UTLR**). See page 108.	Identify T1 receive-line quality problems from the CPE over a longer time frame than the TSR. Available on add/drop units only.
	Far-end Performance Report (**FESR/FELR**). See page 112.	Identify T1 transmit-line quality problems; most useful when the DataSMART and frame switch are several miles apart.
T1 statistical reports	NI Statistical Performance Report (**NSR**). See page 114.	Quickly identify T1 receive-line problems when turning up T1 service.
	TI Statistical Performance Report (**TSR**). See page 114.	Quickly identify T1 receive-line problems from the customer premise equipment (CPE) when turning up T1 service (add/drops).
History reports	Alarm History Report (**AHR**). See page 118.	View the 20 most recent T1 alarm messages.
	Security History Report (**SHR**). See page 119.	View the 10 most recent security violations.
Frame statistical reports	NI/DP Interface Frame Relay Statistical Report (**NDSR**). See page 120.	View statistical counts for data relating to the Network and Data Port interfaces.
	Virtual Circuit Statistical Report (**VCSR**). See page 122.	Monitor unusual frame events and determine whether or not equipment is incorrectly configured.
	VC Availability Report (**VCAR**). See page 126.	View status and statistical counts for data relating to each VC's availability.
Frame utilization report	Virtual Circuit Utilization Report (**VCUR**). See page 124.	Analyze a VC's bandwidth utilization and compare it with the purchased Committed Information Rate (CIR) for that VC.
Frame performance reports	VC Delay Report (**VCDR**). See page 129.	View round-trip delay data of virtual circuits (VCs) in the transmit or receive direction.
	VC Frame Delivered Report (**VDFR**). See page 131.	View statistical counts for delivered frames and octets of virtual circuits in the transmit or receive direction.

The first section of this chapter shows how to access the various command-line reports. The next sections show how to interpret the command-line reports, and the final section shows how to access and interpret reports from the front panel.

Accessing the reports

The DataSMART FrameVision DSU employs two menus for accessing reports: the Reports menu (physical layer) and the Frame Relay Monitoring Reports menu.

Physical Layer reports

To see the Reports menu, enter **R** at the command line.


```
                    REPORTS MENU

UNSR / UNLR         - User NI Short/Long Performance Report
UTSR / UTLR         - User TI Short/Long Performance Report
FESR / FELR         - Far End PRM Short/Long Performance Report
NSR:[z]             - User NI Statistical Performance Report
TSR:[z]             - User TI Statistical Performance Report
                      z = Display Report, then Zero Counts (Optional)
AHR                 - Alarm History Report
SHR                 - Security History Report

PL:<len|style>      - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                      <style> = P (Page Break), M (More), or V (View)
```

TIP
The reports are also available using the DataSMART Installer application shipped with your DataSMART unit.

To display any report, enter the appropriate command from the command line. You do not need any special privilege level.

Some reports have a long or short version. The long version differs from the short version in that it includes a breakdown of the performance information for the previous 24 hours, shown in 15-minute intervals.

Frame Relay Monitoring reports

To see the Frame Relay Monitoring Reports menu, enter **RFRM** at the command line.

```
                FRAME RELAY MONITORING REPORTS MENU

NDSR[:z]        - NI/DP Statistical Report
VCSR[:<vc>[,z]] - VC Statistical Report
                  <vc> = 0..1023, * (All), or O (Other) (Optional)

VCUR[:<vc>[,z]] - VC Utilization Report
VCAR[:<vc>[,z]] - VC Availability Report
VCDR[:<vc>[,z]] - VC Delay Report
VCFR[:<vc>[,z]] - VC Frame Delivered Report
                  <vc> = 0..1023, or * (All) (Optional)

                  <z> = Display Report then Zero Counts (Optional)
```

Formatting the reports

The **PL** command formats all the reports, either for a printer or a terminal. You can set the page length and select either “page break” for output to a printer, or “more prompt” for output to a screen. A page length of 0 disables both page breaks and prompting.

By default, no page length is specified and page breaks and prompting are disabled. If you enter a page length, the command defaults to a “more prompt” (**M**) unless you specify “page breaks” (**P**).

The **PL** command syntax is:

PL:*len*|*style*

len	Specify the page length as **0**, **20** ... **70**. 0 disables page breaks and prompting.
style	Specify **P** for "page break," **M** for "more prompt," or **V** to display the current settings without changing anything.

For example, to fit a report on a 22-line monitor, enter:

PL:22

Any time you change the length or style parameter, a display will show the state of the settings after the change.

Using the Z option

The NI and TI Statistical Reports provide performance data similar to the NI User Report, plus in-service data about total errors counted at the specified interface. The NI/DP Statistical Report displays raw counts of frame error conditions. By using the **Z** option with these report commands, you can clear the error counts whenever the report is displayed. This way, the next time you display the report it will show just the errors accumulated since the last time you displayed the report.

The command syntax is:

NSR [Z]

TSR [Z]

Z	Clears the error counts from the report, once the report is displayed.

Clearing the performance database

Resetting the date or time on the DataSMART using the **ST** or **SD** commands (see "Setting date and time" on page 33) clears the performance data and resets counters. Using the **ZALL** command (see "Zeroing all counters" on page 39) has the same effect, without changing the time.

The **SD**, **ST**, and **ZALL** commands clear data from all reports except the Alarm History Report and the Security History Report.

The following actions will clear data from all reports including the history reports:

- Cycling power to the DataSMART
- Using the **BOOT** command (see "Obtaining new system software" on page 39)
- Resetting the DataSMART to its defaults with the **RSD** command (see "Resetting to default values" on page 41). This command causes you to lose the current alarm history data, performance data, and configuration settings. Use the **RSD** command with caution.

Interpreting the User NI and User TI Reports

The DataSMART monitors the received signal on a T1 line. The User NI Report displays error counts and can be used to determine signal quality.

The DataSMART monitors the received signal on a T1 line for a variety of different error conditions (see "T1 alarms and signal processing" on page 177 for descriptions of errored signal conditions). The DataSMART counts the errors and then uses the count to determine the quality of the one-second interval during which the errors occurred.

For each time interval, the DataSMART tallies the counts and displays the information in the reports. The reports also show the error conditions and whether or not an alarm was present.

The following figure is an example of the User NI Short Performance Report (**UNSR**). The **UTSR** report is very similar.

```
KENTROX DataSMART - USER NI SHORT PERFORMANCE REPORT
NAME: PORTLAND,OR
DATE: OCT 14, 1998              TIME OF DAY: 00:27
STATUS CODES: C=CRC6, B=BPV, L=LOS, O=OOF, E=EER, A=AIS, Y=YEL,
              @=ALARM ACTIVE, T=TEST ACTIVE
SECOND OF INTERVAL: 757 OF 900  COMPLETED INTERVALS: 96 OF 96

                    G.821         G.821  G.821        G.821
              EE      ES    BES    SES    UAS    CSS    DM     STATUS
           ------  -----  -----  -----  -----  -----  ----  ---------
CUR SEC         0      0      0      0      0      0     0       E  @
PRE SEC         0      0      0      0      0      0     0       E  @
CUR 15-MIN   3710      2      2      0     10     18     1  CB   E  @
PRE 15-MIN     18      5      0      5     15     16     0   BL  E  @
CUR 24-HR      80     13      0     13     15     75     0  CBLOE  @
```

What to look for

Real or potential problems with T1 service are indicated by:

- Nonzero results in the performance measurement columns (EE, ES, BES, SES, UAS, CSS, and DM) indicate seconds (or minutes) when errors occurred.
- Characters in the Status column indicate error or test conditions, and the @ symbol appears if the error conditions persisted long enough to cause alarms.

For details, see page 110.

Time intervals in the performance report

The report shows the performance data for the current second, the previous second, the current 15-minute period, the previous 15-minute period, the current day, and the previous seven days.

Each day is broken into ninety-six 15-minute intervals. Interval one starts at 00:00 (midnight), interval two at 00:15, interval three at 00:30, and so on.

CUR 15-MIN refers to the performance data tabulated so far for the 15-minute interval. For instance, in the previous figure, the third row shows the performance for the 15-minute interval starting at 00:15 (notice that the time of day is 00:27).

Each 15-minute interval consists of 900 seconds. The field in the header labeled "SECOND OF INTERVAL" shows how many seconds into the interval the measurement extends. In the example, the data has been collected for 757 seconds of the current interval.

In a report, CUR 24-HR refers to a rolling 24-hour period. In other words, it is the previous ninety-six 15-minute intervals. The field labeled "COMPLETED INTERVALS" indicates whether or not the DataSMART has been running for the full ninety-six intervals that make up a 24-hour day. Unless the DataSMART was recently restarted, the completed intervals display should always read "96 OF 96." The 24-hour count may show less than ninety-six 15-minute intervals if it was cleared within the last 24 hours.

The report also shows the performance data for each of the last seven days, if the DataSMART has been powered up for seven days; otherwise, it shows the data collected since the DataSMART was last powered up. For instance, if the DataSMART has only been powered up for 48 hours, the report will only have a listing for two days, since only two days have been completed so far.

If one of the time intervals shows a row of dashes (-), that means that either the DataSMART was powered down during that period or data has not yet been collected for that period.

A zero (0) indicates that the unit was collecting data and for that field the count was zero.

Time intervals and the long report

The long report (use the **UNLR** or **UTLR** command) shows the same information as the short report and also includes performance data for each complete 15-minute interval in the current 24 hours (that is, the previous ninety-six 15-minute intervals). If not all of the 15-minute intervals are listed, it means the DataSMART has not been on for 24 hours. A dash displayed in a field means that the unit was powered down for that period.

The following figure shows the additional information provided by the long version of the User NI Report (**UNLR**).

```
TIME ACCUMULATED
    17:30        0      0      0      0      0      0     0
    17:15        0      0      0      0      0      0     0
    17:00        0      0      0      0      0      0     0
    16:45        0      0      0      0      0      0     0
    16:30       18      5      0      5     15     16     0   BL E  @
    16:15       62      8      0      8      0     59     0  C LO   @
```

For each time interval there are eight types of performance measurements. These measurements are described below.

Field header	Definition
EE	This field shows the number of error events (EEs) that have occurred, up to a maximum of 999,999. If the line uses ESF framing, the following error conditions cause a single EE to be counted: a transition to the LOS condition a transition to the AIS condition a transition to the OOF condition a second with a controlled slip (also referred to as a frame slip)[1] a BPV error a CRC6 error If the line uses SF framing, an EE is the number of BPVs per second.
ES	This field lists the number of errored seconds (ESs) that have occurred. If the line uses ESF framing, an ES is any second that is not a UAS and contains: an LOS condition, or an AIS condition, or an OOF condition, or one or more CRC6 or BPV errors. If the line uses SF framing, an ES is any second with a BPV, LOS, AIS, or OOF. Controlled slips do not result in ESs (as per CCITT G.821 paragraph 1.8). When a single LOS, AIS, or OOF condition lasts for several seconds, it counts as a single EE, not as several ESs and SESs.
BES	This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400. A BES is any second that is not a UAS and contains: no LOS, AIS, or OOF conditions, and between 2 and 319 (inclusive) EEs.
SES	This field lists the number of severely errored seconds (SESs) that have occurred, up to a maximum of 86,400. An SES is any second that is not a UAS and contains: an LOS condition, or an AIS condition, or an OOF condition, or 320 or more EEs.
UAS	This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.
CSS	This field lists the number of controlled slip seconds (CSSs) that have occurred, up to a maximum of 86,400. A controlled slip second is any second and contains one or more controlled slips (see also the definition for ES). CSSs are accumulated during unavailable seconds (UASs).
During any one-second time period, the above error events can occur in various combinations. The possible combinations are: no errors; ES; CSS; ES and CSS; ES and BES; ES and BES and CSS; ES and SES; ES and SES and CSS; UAS; UAS and CSS.	

Field header	Definition
DM	This field lists the number of degraded minutes (DMs) that have occurred, up to a maximum of 1,440. A DM is a sixty-second non-UAS and non-SES period that contains 49 or more CRC6 or BPV errors (ESF framing) or 49 or more bipolar violations (SF framing).
STATUS	This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below. In order of severity, the conditions are: **L** An LOS condition has occurred, but has not necessarily integrated to an alarm state. Inbound traffic has stopped. **O** An OOF condition has occurred, but has not necessarily integrated to an alarm state. Inbound traffic has stopped. **A** An AIS condition (but not necessarily an alarm) has occurred. Inbound traffic has stopped. **Y** A yellow alarm has been detected. Outbound traffic may have stopped. **E** An Excessive Error Rate (EER) condition (but not necessarily an alarm) has occurred. This condition can occur only if the EER alarm is enabled. Inbound traffic contains errors. **@** One of the preceding conditions has persisted long enough to cause an alarm state. **B** For both ESF and SF, a “B” is displayed if a BPV occurs. **C** If ESF is enabled, a “C” is displayed if a CRC6 error occurs. **T** There is a (loopback, code generation, or BERT) test active on the DataSMART.

[1] A controlled slip is declared when the DataSMART detects an accrued timing difference of exactly one frame between the transmitted and received data streams, resulting in the deletion or addition of a single frame in the received data stream.

Interpreting the Far-end Report

*The **FESR** and **FELR** commands display the performance history of the received signal at the far-end network interface. In Frame Relay networks, the far-end device is typically a Frame Relay switch, which exchanges performance data through Performance Report Messages (PRMs) over the ESF facility data link.*

Because the Far-end Reports are based on PRMs, the far-end device (the Frame Relay switch in a Frame Relay network) must be T1.403 compatible. Also, PRM generation must be enabled in the near-end and far-end devices, and the T1 line's framing format must be ESF. (Use the **EPRM** command to enable PRM generation in the DataSMART and use the **NESF** command to enable ESF framing format.)

The Far-end Reports show you T1 line performance as seen by the device on the far end of the circuit, without the need to connect to the far-end device directly. Using the Far-end Reports and the NI Statistical Reports (see "Interpreting the User NI and User TI Reports" on page 108) gives you a clear picture of T1 performance in both the transmit and receive directions.

The figure below shows an example of a short version of the Far-end Report. Notice that it is the same as a User NI Report except for the status codes described in the header and listed in the status column.

```
KENTROX DataSMART - FAR END PRM SHORT PERFORMANCE REPORT
NAME: PORTLAND,OR
DATE: OCT 14, 1998              TIME OF DAY: 10:53
STATUS CODES: C=CRC6, V=LCV, F=FRAME BIT ERR, E=SEVERE FRAME BIT,
              S=SLIP, P=PAYLOAD LOOP BACK, M=MISSED 4 PRM, N=NO POWER
SECOND OF INTERVAL: 495 OF 900  COMPLETED INTERVALS: 1 OF 96

                    G.821         G.821  G.821        G.821
              EE      ES    BES    SES    UAS    CSS    DM     STATUS
            ------  -----  -----  -----  -----  -----  ----  ----------
CUR SEC        319      1      1      0      0      0     0  C VF
PRE SEC        319      1      1      0      0      0     0  C VF
CUR 15-MIN    6776     59     59      0      0      0     1  C VFE  M
PRE 15-MIN       -      -      -      -      -      -     -
CUR 24-HR        -      -      -      -      -      -     -
```

What to look for and how to interpret time intervals

The items to look for in the Far-end Reports and User NI Reports are the same, except the Far-end Reports do not include alarm states. Also, time intervals are the same in the Far-end Reports and User NI Reports. See page 109.

The following table describes the performance data displayed in the Far-end Report.

Field header	Description
EE	This first field lists the number of error events (EEs) that have occurred, up to a maximum of 999,999. Only CRC6 errors are used to calculate error events. The PRM message does not provide exact counts of CRC6 error events. Instead it uses 6 bits to indicate that the error rate fell within a certain range; then the highest number in the range (except for the last range, as noted below) is used as the error count in the Far-end Report as follows:

Field header	Description
EE (continued)	1 CRC6 error-per-second counts as one EE 2 to 5 CRC6 errors-per-second count as 5 EEs 6 to 10 CRC6 errors-per-second count as 10 EEs 11 to 100 CRC6 errors-per-second count as 100 EEs 101 to 319 CRC6 errors-per-second count as 319 EEs 320 or more CRC6 errors-per-second count as 333 EEs
ES	This field lists the number of errored seconds (ESs) that have occurred during the time interval, up to a maximum of 86,400. An ES is any second that is not a UAS and contains one or more CRC6 errors.
BES	This field lists the number of bursty errored seconds (BESs) that have occurred during the time interval, up to a maximum of 86,400. A BES is any second that is not a UAS and contains between 2 and 319 (inclusive) CRC6 errors.
SES	This field lists the number of severely errored seconds (SESs) that have occurred during the time interval, up to a maximum of 86,400. An SES is any second that is not a UAS and contains 320 or more CRC6 errors.
UAS	This field lists the number of unavailable seconds (UASs) that have occurred, up to a maximum of 86,400. A UAS state is declared when ten consecutive SESs occur. The ten SESs are subtracted from the SES count and added to the UAS count. Subsequent seconds are accrued to the UAS count until the UAS state is cleared. The UAS state is cleared when ten consecutive non-SESs occur. When that happens, the consecutive ten non-SESs are subtracted from the UAS count.
CSS	This field lists the number of controlled slip seconds (CSSs) that have occurred during the time interval, up to a maximum of 86,400. A controlled slip second is any second that contains one or more controlled slips (see also the definition for ES). CSSs are accumulated during unavailable seconds (UASs).
During any one second time period, the above error events can occur in various combinations, which are: no errors; ES; CSS; ES and CSS; ES and BES;ES and BES and CSS; ES and SES; ES and SES and CSS; UAS; UAS and CSS.	
DM	This field lists the number of degraded minutes (DMs) that have occurred during the time interval, up to a maximum of 1,440. A degraded minute is a sixty-second non-UAS and non-SES period that contains 49 or more CRC6 errors (ESF framing) or 49 or more bipolar violations (SF framing).
Status	This field shows the type of errored conditions that occurred during the time interval. The conditions are indicated by a single character as described below: **F** A frame synchronization bit error has occurred in the received network signal. A frame synchronization bit error occurs when an error in the framing-bit pattern is received. **E** A severely-errored framing event has occurred in the received network signal. A severely-errored framing event occurs when two or more framing-bit-pattern errors occur within a 3-millisecond period. **C** A CRC6 error has been detected in the received T1 signal. **V** A line code violation condition has occurred in the received network signal. A line code violation occurs when a bipolar violation that is not part of a zero-substitution code is received. **S** A controlled slip has occurred at the received network signal. A controlled slip event occurs when there is a replication or deletion of a T1 frame by the receiving network interface. **P** A payload loopback is active on the network interface. **M** No PRMs have been received for four or more consecutive seconds. Each PRM contains information for four consecutive seconds, so no data is lost if up to three PRMs are missing.

Interpreting the NI and TI Statistical Reports

*The **NSR** and **TSR** commands display statistical reports of the received signal on the network interface and terminal interface respectively. The **NSR Z** and **TSR Z** commands display the statistical reports, and then clear the error data.*

Using the NI Statistical Report when you first turn up a new T1 line will give you a snapshot of T1 service quality in the receive direction. For more detail, run the User NI Performance Reports (see page 108). The TI Statistical Report is similar. It shows the quality of the connection to customer premise equipment connected to the DataSMART.

A statistical report has two parts. The first part is a statistical summary of the recent performance history of the received signal. The second part is an in-service performance measurement of the received signal. The following figure shows an example of an NI Statistical Report (**NSR**).

```
KENTROX DataSMART - USER NI STATISTICAL PERFORMANCE REPORT
NAME: PORTLAND,OR
DATE: OCT 14, 1998              TIME OF DAY: 16:48
            |-------------- G.821 ---------------|
            %AS    %EFS     %ES    %SES     %DM    %BES    %CSS
            ------  ------  ------  ------  ------  ------  ------
CUR 15-MIN  100.00  100.00  0.0000  0.0000  0.0000  0.0000  2.0304
PRE 15-MIN  98.888  99.775  0.2247  0.0000  6.6666  0.2247  2.0224
CUR 24-HR   99.073  99.439  0.5609  0.4861  2.2222  0.0747  3.4779
START OF TEST:  DATE: FEB 14, 1997
                TIME: 16:00
PERFORMANCE MEASUREMENT            COUNT
----------------------------   ----------
ESF ERRORS                          11718
CRC6 ERRORS                          3693
OUT OF FRAME ERRORS                  8025
FRAME BIT ERRORS                       18
BIPOLAR VIOLATIONS                  14175
CONTROLLED SLIPS                      155
YELLOW ALARM EVENTS                     0
AIS EVENTS                              0
LOSS OF FRAME EVENTS                    1
LOSS OF SIGNAL EVENTS                   3
```

What to look for

To test NI performance for a specified time period, use the **NSR Z** command to generate a report and clear the data. Then periodically use the **NSR** command to check performance over time. Trouble indicators are:

- Values in the %AS and %EFS columns that are under 100 percent
- Nonzero values in the %ES, %SES, %DM, %BES, and CSS columns
- Nonzero counts in the Performance Measurement area (for definitions of the performance measurements, see page 117)

The report's statistical summary

The statistical summary shows statistical percentages for the current 15-minute interval, the previous 15-minute interval, the current 24-hour interval, and each of the previous seven days. These intervals are the same as those in the User NI Report; see "Time intervals in the performance report" on page 109 for a description.

The percentages are computed from the counts stored in the performance database for the User NI Report. They are computed using the concept of an "available second." In the formulas defined below, you will see the variable Sec_avail. An available second is simply any second that is not an unavailable second:

Sec_avail = Sec_total - UAS

Specifically, the number of available seconds for any time period is simply the number of total seconds for the time period (900 for 15 minutes, 86,400 for 24 hours) minus the number of UAS seconds. See "UAS" on page 110 for a definition of an unavailable second.

Any time "Sec_avail" is zero for a time period and the formula for computing the percentage uses "Sec_avail" in a denominator, a series of dashes is displayed as the result instead of a numerical value.

The following is a list of the seven fields in the statistical summary and the formulas used to compute their values.

Field header	Description
%AS	This field lists the percentage of available seconds (%AS) for the time interval. The formula for this statistic is: %AS = (Sec_avail / Sec_total) x 100
%EFS	This field lists the percentage of error-free seconds (%EFS) for the time interval. An error-free second is any available second that was not an errored second. The formula is: %EFS = ((Sec_avail - ES) / Sec_avail) x 100 where ES is the number of errored seconds for the time interval.
%ES	This field lists the percentage of errored seconds (%ES) for the time interval. The formula for this statistic utilizes ES, where ES is the number of errored seconds. The formula is: %ES = (ES / Sec_avail) x 100 Note that the sum of %EFS and %ES should be 100%.
%SES	This field lists the percentage of severely errored seconds (%SES) for the time interval. The formula for this statistic utilizes SES, where SES is the number of severely errored seconds (using the same definition as for the User NI Report; see page 110). The formula is: %SES = (SES / Sec_avail) x 100
%DM	This field lists the percentage of degraded minutes (%DM) for the time interval. The formula for this statistic utilizes DM, where DM is the number of degraded minutes (using the same definition as for the User NI Report; see page 110). The formula is: %DM = (DM / ((Sec_avail / 60) rounded to next higher integer)) x 100
%BES	This field lists the percentage of bursty errored seconds (%BES) for the time interval. The formula for this statistic utilizes BES, where BES is the number of bursty errored seconds for the time interval (using the same definition as for the User NI Report; see page 110). The formula is: %BES = (BES / Sec_avail) x 100
%CSS	This field lists the percentage of controlled slip seconds (%CSS) for the time interval. The formula for this statistic utilizes CSS, where CSS is the number of controlled slip seconds for the time interval (using the same definition as for the User NI Report; see page 110). The formula is: %CSS = (CSS / Sec_avail) x 100

The statistical report's in-service performance measurement

The second part of this report displays counts of various error conditions in the received network signal. These are just raw counts, not percentages. The data for this display is kept in registers separate from the registers used for other reports. You can reset the counts at any time. Resetting the count does not affect performance information (including the information in the first part of the statistical report). The error counts are useful for running an in-service test on the network line.

To run an in-service test on the network interface, use these steps:

1. Issue the **NSR** or **TSR** command using the **Z** option to clear (zero-out) the error counts.

   NSR Z

   This displays the statistical report, showing the error counts at the time the command was issued, and then clears the error data.

2. Wait the desired time interval.

3. Issue the NSR (or TSR) command again.

   This displays the error counts accumulated since the time you cleared the error counts.

   The figure below shows an example of an in-service performance measurement. The header shows the start of the test, which is the time that the error counts were last cleared. Below that are two columns, listing the type of error condition and a corresponding error count. The maximum value that may appear in any count field is 2^{32}-1 (4,294,967,295). When this limit is reached, the count wraps to zero (0).

```
KENTROX DataSMART 698 - USER NI STATISTICAL PERFORMANCE REPORT
NAME: PORTLAND,OR
DATE: OCT 14, 1998              TIME OF DAY: 16:48
            |-------------- G.821 ---------------|
            %AS    %EFS     %ES    %SES     %DM    %BES    %CSS
            ------  ------  ------  ------  ------  ------  ------
CUR 15-MIN  100.00  100.00  0.0000  0.0000  0.0000  0.0000  2.0304
PRE 15-MIN  98.888  99.775  0.2247  0.0000  6.6666  0.2247  2.0224
CUR 24-HR   99.073  99.439  0.5609  0.4861  2.2222  0.0747  3.4779
START OF TEST:  DATE: OCT 14, 1998
                TIME: 16:00
PERFORMANCE MEASUREMENT            COUNT
-----------------------------   ----------
ESF ERRORS                         13016
CRC6 ERRORS                        11215
OUT OF FRAME ERRORS                 2105
FRAME BIT ERRORS                      18
BIPOLAR VIOLATIONS                 14175
CONTROLLED SLIPS                     155
YELLOW ALARM EVENTS                    0
AIS EVENTS                             0
LOSS OF FRAME EVENTS                   1
LOSS OF SIGNAL EVENTS                  3
```

Interface statistical report

Counts of the following error conditions are maintained and displayed in response to the **NSR** or **TSR** command:

- ESF Errors (ESF only): this event occurs when a frame contains a CRC error, an OOF error, or both.
- CRC6 Errors (ESF only): this error occurs when the CRC checksums calculated for a frame at the transmitting and receiving ends are different.
- Out of Frame Errors (ESF and SF): two or more framing bit errors have been received within a 3-millisecond period.
- Frame Bit Errors (ESF and SF): errors have been received in the framing bits at a rate of less than 1 every 3 milliseconds.
- Bipolar Violations (ESF and SF): this event is any bipolar violation generated in error (not including intentional bipolar violations generated by B8ZS coding).
- Controlled Slips: this event is the addition or deletion of a single frame in the received data stream, due to a timing difference of exactly one frame between the transmitted and received data streams. Make sure you are using one and only one timing source.
- Yellow Alarm Events: this event is a transition from the condition of “not receiving yellow” to the yellow condition.
- AIS Events: this event is a transition from the condition of “not receiving AIS” to the AIS condition.
- Loss of Frame Events: this event is a transition from the framed condition to the OOF condition.
- Loss of Signal Events: this event is a transition to the LOS condition. See “Examining system status” on page 139.

For more detailed definitions, see page 110, “Troubleshooting tree” on page 143, or the Glossary.

Interpreting the Alarm History Report

*The Alarm History Report (use the **AHR** command) shows the last 20 alarm messages. The alarm messages in the report are the same messages sent to the control port device when the control port alarm messages are enabled and configured for ASCII format.*

Alarm messages are generated by physical-layer alarm states on the network interface or data port. A message is added to the report every time the network interface or data port changes to a different alarm state. The "Alarm Cleared" message is not issued unless all alarms on that line are cleared. The report logs up to twenty messages, most recent first. Once the report reaches twenty messages, each new alarm message causes the oldest message to be dropped.

See "Monitoring alarm messages" on page 137 for a full list of the types of alarm messages that can appear in this report and their meanings.

TIP
Using DataSMART Installer, this information can be saved to disk for later use.

The alarm messages are always displayed in user format (ASCII text).

Alarm messages always appear in the Alarm History Report, even if alarm messages are disabled with the **DAM** command in the Alarm Configuration menu.

Information in the Alarm History Report is not cleared when an **ST**, **SD**, or **ZALL** command is executed.

The following actions clear the Alarm History Report:

- Power cycling the DataSMART
- Executing the **RSD** command (see "Resetting to default values" on page 41)
- Executing the **BOOT** command (see "Obtaining new system software" on page 39)

An example of the Alarm History Report is shown below.

```
SET ALM OCT.14,1998 16:37 TI EER PORTLAND,OR
SET ALM OCT.14,1998 16:37 NI EER PORTLAND,OR
SET ALM OCT.14,1998 16:36 TI LOS PORTLAND,OR
CLR ALM OCT.14,1998 16:32 NI     PORTLAND,OR
CLR ALM OCT.14,1998 16:22 TI     PORTLAND,OR
SET ALM OCT.14,1998 16:22 TI OOF PORTLAND,OR
SET ALM OCT.14,1998 16:22 TI LOS PORTLAND,OR
SET ALM OCT.14,1998 16:16 NI EER PORTLAND,OR
SET ALM OCT.14,1998 16:16 NI LOS PORTLAND,OR
SET ALM OCT.14,1998 16:16 NI EER PORTLAND,OR
CLR ALM OCT.14,1998 16:16 NI     PORTLAND,OR
SET ALM OCT.14,1998 16:15 NI LOS PORTLAND,OR
CLR ALM OCT.14,1998 16:02 NI     PORTLAND,OR
SET ALM OCT.14,1998 16:01 NI LOS PORTLAND,OR
```

Interpreting the Security History Report

*The Security History Report (use the **SHR** command) shows the last 10 events that might indicate unauthorized attempts to access the DataSMART.*

The report includes three types of events:

- An incorrect Telnet password has been entered (Telnet Password).
- The DataSMART has read or written an incorrect SNMP community string (SNMP Rd CommString or SNMP Wr CommString).
- The DataSMART has received an IP packet from a host whose IP address is not on the Source Screening Address list (IP Screen).

The report logs up to 10 events, most recent first. Once the report reaches 10 events, each subsequent message causes the oldest event to be dropped.

The IP address of the device which caused the security event is listed under "Comments."

You can configure the SNMP agent to send an SNMP Authentication Trap whenever one of these security events occurs. To configure these traps, see "Configuring for SNMP" on page 90.

Information in the Security History Report is not cleared when an **ST**, **SD**, or **ZALL** command is executed.

The following actions clear the Security History Report:

- Power cycling the DataSMART
- Executing the **RSD** command (see "Resetting to default values" on page 41)
- Executing the **BOOT** command (see "Obtaining new system software" on page 39)

An example of the Security History Report is shown below.

```
Date/Time          Security Event        Comments
-----------------  --------------------  ---------------------------
OCT.14,1998 11:58  Telnet Password       Src IP Addr: 192.0.2.1
OCT.14,1998 11:52  SNMP Wr CommString    Src IP Addr: 192.0.2.1
OCT.13,1998 10:51  IP Screen             Src IP Addr: 192.0.2.11
```

Interpreting the NI/DP Interface Frame Relay Statistical Report

The NDSR report displays information about the condition and usage of the network interface and data port.

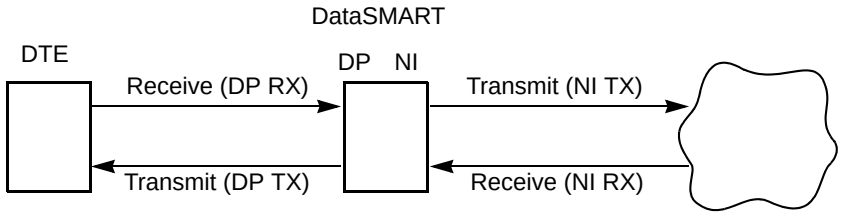
Headers in all statistical reports

The header of any frame statistical report contains information about the length of time the DataSMART unit has been gathering data for that report:

- **Start of report** indicates the date and time that the report data was last zeroed out. All statistical counters began counting at this time. It appears only if you have entered the date and time using the **SD** and **ST** commands after powering up.
- **Current date/time** displays the current date and time. It appears only if you have entered the date and time using the **SD** and **ST** commands after powering up.
- **Report duration** displays the total amount of time that the counters in the report have been collecting data (the total elapsed time since the data was last zeroed out). This information is displayed even if the date and time were not entered at power-up.

Availability statistics for the NI and DP

For the NDSR report, the transmit and receive directions for both the network interface and data port are measured from the point of view of the DataSMART.



The following figure shows an example of an NI/DP Statistical Report.

```
KENTROX DataSMART 696 - NI/DP Statistical Report
NAME: PORTLAND, OR
Start of report:    Date: NOV 10, 1998    Time: 07:32
Current date/time:  Date: NOV 17, 1998    Time: 18:25
Report duration:       7 days 10 hrs 52 min 21 secs

                          NI             DP
                     ----------     ----------
Available Seconds    1234567890     1234567890
Test Seconds         1234567890     1234567890
Alarm Seconds        1234567890     1234567890
Total Seconds        1234567890     1234567890

                       NI: Tx     NI: Rx     DP: Tx     DP: Rx
                     ----------  ----------  ----------  ----------
Frames               1234567890  1234567890  1234567890  1234567890
Octets               1234567890  1234567890  1234567890  1234567890
IP Mgmt Frames       1234567890  1234567890  1234567890  1234567890
IP Mgmt Octets       1234567890  1234567890  1234567890  1234567890
FPING Frames         1234567890  1234567890
FPING Octets         1234567890  1234567890
FR Header Invalid                1234567890              1234567890
FR Frame Too Long                1234567890              1234567890
HDLC Errors                      1234567890              1234567890
```

The following is a list of the fields in the statistical summary and their definitions. Most fields collect data only when the unit is in Monitor mode, but some also collect data when the unit is in Transparent mode. Not all fields contain data.

Field header	Description
The first section contains data relating to the availability of each interface.	
NI Available Seconds	Seconds the interface is operationally available. The time in seconds the NI is not in alarm or NI test state. Where NI test state defines that time when loopbacks are initiated by local loop commands.
NI Test Seconds	The time in seconds that the NI is in a test mode due to Line Loopback or Payload Loopback being set or a test code being sent.
NI Alarm Seconds	The time in seconds this interface is in an alarm state.
NI Total Seconds	Seconds the interface is administratively available (i.e., a user has not disabled it).
DP Available Seconds	Seconds the interface is operationally available. The time in seconds the data port is available as defined by configuration and/or DP LOS.
DP Test Seconds	The time in seconds that the data port is in a test mode due to a DPT loopback being set.
DP Alarm Seconds	The time in seconds that the data port is in the alarm state as defined by DP LOS.
DP Total Seconds	Seconds the data port is administratively available.
Data is monitored in both the transmit and receive directions for each interface, although not all measurements are relevant in both directions. Tx and Rx are from the perspective of the port (either NI or DP). For example, “DP: Rx” and “NI: Tx” represent the same stream of data flowing from the DTE (router) towards the network (switch).	
Frames*	The number of HDLC frames.
Octets*	The number of non-flag octets.
IP Mgmt Frame*	The number of HDLC frames that are IP management packets to or from this unit.
IP Mgmt Octets*	The number of octets within IP management frames to or from this unit.
FPING Frames*	The number of HDLC frames that are FPING packets to or from this unit.
FPING Octets*	The number of octets within FPING frames to or from this unit.
FR Header Invalid*	The number of Frame Relay frames whose header does not contain either 2, 3 or 4 octets (as indicated by the EA bits). (NI Rx and DP Rx.)
FR Frame Too Long*	The number of frames that are too large to be received by the interface (65,535 bytes). (NI Rx and DP Rx.)
HDLC Errors*	The number of HDLC errors. This includes CRC errors, aborts, and non-octet aligned frames (frames whose total bit length is not divisible by 8). (NI Rx and DP Rx.)

* Valid in Monitor Mode only.

Displaying the report from the command line

Use the following command:

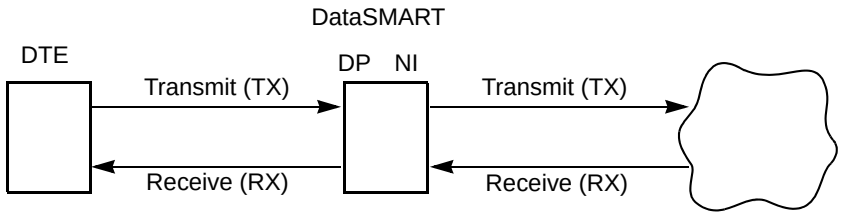
NDSR[:**Z**]

Z Clear the information in the report after displaying it. Z clears all the values and resets the “Start of Test” date and time.

Displaying and interpreting the VC Statistical Report

The VCSR report displays statistical counts for data relating to Frame Relay VC traffic. All measurements are from the perspective of the NI.

The Virtual Circuit Statistical Report (**VCSR**) monitors unusual frame events and helps you determine whether or not equipment is incorrectly configured. The unit measures each VC in the transmit and receive direction. These directions apply to both the VCSR and the Virtual Circuit Utilization Report (page 124).



The following figure shows an example of a VC Statistical Report.

```
KENTROX DataSMART 696 - VC Statistical Report - All VCs
NAME: PORTLAND, OR
Start of report:    Date: NOV 10, 1998    Time: 07:32
Current date/time:  Date: NOV 17, 1998    Time: 18:25
Report duration:       7 days 10 hrs 52 min 21 secs

DLCI/DIR     OCTETS     FRAMES       DE        FECN       BECN
---------  ---------- ---------- ---------- ---------- ----------
0     RX      890        890        90         0          0
0     RX      890        7890       90         90         90
56    RX      890        7890       90         90         90
56    TX      7890       67890      90         90         90
234   RX      7890       67890      90         90         90
234   TX      7890       67890      90         90         90
```

What to look for

- **DLCIs 0 and 1023** carry link management traffic between the Frame Relay switch and the router or FRAD. These DLCIs carry no user data.
- **Discard eligible (DE)** indicates traffic that exceeds the Committed Information Rate (CIR). Traffic going in the Transmit direction may be discarded if the network is congested. The router or Frame Relay switch may have tagged the affected frames.
- **Forward explicit congestion notification (FECN)** and **backward explicit congestion notification (BECN)** indicate general Frame Relay congestion which may have caused application delays in your data traffic.

The following is a list of the fields in the statistical summary and their definitions. All measurements are valid in the receive and transmit directions.

Field header	Description
DLCI/DIR	The VC and direction the data was measured on. Direction can be RX or TX. The display for each VC will contain an RX and TX component.
FRAMES	The number of frames measured on VC. Valid for RX and TX.
OCTETS	The number of data octets measured on VC (does not include CRC, address field). Valid for RX and TX.
DE	The number of frames measured on VC with the DE bit set. Valid for RX and TX.
FECN	The number of frames measured on VC with the FECN bit set. Valid for RX and TX.
BECN	The number of frames measured on VC with the BECN bit set. Valid for RX and TX (i.e., included this VC in full status response messages).

Displaying the report from the command line

Use the following command:

VCSR[:*vc* [**Z**]]

vc	Enter the virtual circuit ID, a number from 1 to 1023, or ***** to view data for all VCs going through the unit.
Z	Clear the information in the report after displaying it. Z clears all the values and resets the “Start of Test” date and time.

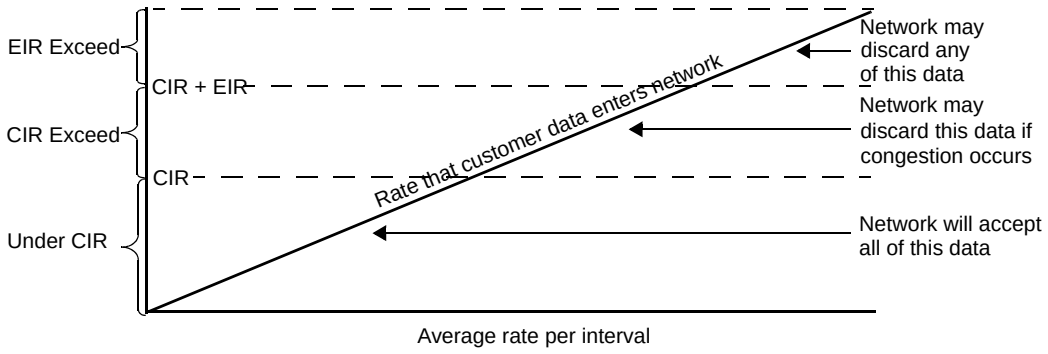
Displaying and interpreting the VC Utilization Report

*The Virtual Circuit Utilization Report (**VCUR**) displays statistical counts for intervals in which a virtual circuit's bandwidth utilization exceeds the committed information rate (CIR) and excess information rate (EIR). The information in this report can identify whether the CIR and EIR are adequate for your application needs.*

When Frame Relay service is purchased, the customer and service provider agree on three parameters that affect network performance and the cost of the service:

- The *access rate*, which is the maximum rate at which the customer can send data into the Frame Relay network. For Frame Relay over full T1, this is 1536000 bits per second. Frame Relay networks don't assume the customer will use bandwidth at the access rate all the time.
- The *committed information rate (CIR)*, which is the rate at which the service provider agrees to accept and deliver data from the customer. The CIR is less than or equal to the access rate.
- The *excess information rate (EIR)*, which is a rate over and above the CIR. If the customer sends bursts of data in excess of the CIR, the EIR determines whether the network accepts and forwards the data that exceed the CIR.

If the customer generates bursts of data in the "CIR Exceed" range (see the figure below), the service provider agrees to accept that data and to make its "best effort" to forward the data. If any switch in the network is momentarily congested, the network may drop packets that exceed the CIR. If the customer sends data at a rate in the "EIR Exceed" range, the service provider has no obligation to accept that data. The figure below shows what can happen to customer data that enters a Frame Relay network at increasingly higher rates.



For example, if the negotiated CIR is 128 kbps and the EIR is 128 kbps, the network accepts and forwards all customer data sent at 128 kbps or slower. Bursts from 128 to 256 kbps will go through the network unless a switch in the network encounters congestion and drops the excess data. Any data bursts in excess of 256 kbps can be discarded by the network.

If you are experiencing slow application response, check the "Excess CIR" and "Excess EIR" columns of the VC Utilization Report. The network may be dropping packets, forcing your router to retransmit them and thus increasing overall response time. A good rule

of thumb is the CIR should be equal to, or slightly higher than, the average rate at which the customer sends data into the Frame Relay network.

You can fix the problem by renegotiating the VC bandwidth, for example, increasing the CIR from 128 kbps to 384 kbps. The EIR (or B_e, a related measurement) is usually tied to the CIR when you purchase it. Almost every router views the access pipe as always available at the maximum bandwidth.

To set the CIR and EIR, see "Setting the CIR and EIR for a VC" on page 101.

The following figure shows an example of a VC Utilization Report.

```
KENTROX DataSMART 696 - VC Utilization Report - ALL VCs
NAME: PORTLAND, OR
Start of report:    Date: OCT 14, 1998    Time: 07:32
Current date/time:  Date: OCT 21, 1998    Time: 18:25
Report duration:       7 days 10 hrs 52 min 21 secs

DLCI/DIR     CIR     EIR    Octet>CIR  Octet>EIR  Frames>CIR Frames>EIR
---------  ------- -------  ---------- ---------- ---------- ----------
  34   RX   128000  128000      121388      58387       4000       4000
  68   TX   256000  256000       93490      21289       1000       1000
 105   TX   384000  384000           0          0          0          0
```

Virtual circuits and the VC Utilization Report

The fields in the VC Utilization Report are:

Field header	Definition
DLCI/DIR	This is the VC and direction the data was measured on. Direction can be RX or TX. It is a number between 1 and 1023.
CIR	This field contains the configured CIR for this VC, in bits per second. CIR can range from 0 (the default) to 1536000. You negotiate this rate when purchasing Frame Relay service. To set or change the CIR, use the **VCMOD** command.
EIR	This field contains the configured EIR for this VC, in bits per second. EIR can range from 0 to 1536000 (the default). It is usually determined for you when you purchase Frame Relay service. To set or change the EIR, use the **VCMOD** command.
Octet > CIR	This field contains the number of octets transmitted during the intervals counted in "CIR Exceed."
Octet > EIR	This field contains the number of octets transmitted during the intervals counted in "EIR Exceed."
Frames > CIR	This field contains the number of frames in which an octet exceeded CIR during the evaluation interval.
Frames > EIR	This field contains the number of frames in which an octet exceeded EIR during the evaluation interval

Displaying the report from the command line

Use the following command:

VCUR[:*vc* [**Z**]]

vc	Enter the virtual circuit ID, a number from 1 to 1023, or ***** to view data for all VCs going through the unit.
Z	Clear the information in the report after displaying it. **Z** clears all the values and resets the "Start of Test" date and time.

Displaying and interpreting the VC Availability Report

The VCAR report displays status and statistical counts detailing the availability of each VC.

The following figure shows an example of a VC Availability Report.

```
KENTROX DataSMART 698 - VC Availability Report - All VCs
NAME: PORTLAND,OR
Start of report:    Date: AUG 10, 1998    Time: 07:32
Current date/time:  Date: AUG 17, 1998    Time: 18:25
Report duration:       0 days 21 hrs 16 min 11 secs

                                  NI          DP
                              ----------  ----------
Physical Available Seconds           33          31
Link Mgmt Available Seconds           0           0

FRLM= LMI      T391=10 N391= 2 N392= 2 N393= 4
STATE: Router and Switch are UP
SPOOFING: Inactive
Spoofing Events: As Service= 1             As Customer= 1
Spoofed Seconds: As Service= 6             As Customer= 28

                        ACTIVE       INACTIVE     #INACTIVE
DLCI   STATUS           SECONDS      SECONDS      TRANSIT
----   -------------   ----------   ----------   ----------
10     ACTIVE               76567            6            1
20     ACTIVE               76567            6            1
40     ACTIVE               76567            6            1
50     ACTIVE               76567            6            1
200    ACTIVE               76567            6            1
```

The fields in the VC Availability Report are:

Field header	Definition
The first section contains the counts, in seconds, for physical and link management availability for the network and data port.	
Physical Available Seconds	Defines the number of seconds each interface has been physically available. For the NI, this means no LOS, OOF, AIS or active test has been detected on the NI. For the Data Port, this means no LOS has been detected on the DP.
Link Management Seconds	Defines the number of seconds each interface has been declared active based on link management messages. For the NI, this means that a status message was received, or no enquiry was received (in which case we don't know the state of the switch, so we count it as available). For the DP, this means that the router is sending enquiries.
The next section contains the configuration parameters relating to FRLM.	
FRLM	Defines the FRLM protocol. Values are "Annex D," "Annex A," and "LMI."
T391	Defines the number of seconds between successive status enquiry intervals. Values range from 5-30. The default is 10.
N391	Defines the number of T391 intervals before a full status enquiry message is sent. Values range from 1 to 255 seconds. The default is 6.
N392	Defines the number of unanswered status enquiries the unit will accept before declaring the interface down. Values range from 1 to 10 enquiries. N392 must be less than or equal to N393. The default is 3.
N393	Defines the number of status polling intervals (T391) over which the error threshold is counted. N393 must be greater than or equal to N392. The default is 4.

Field header	Definition
STATE	Values are: **Detecting**—unit is still watching the line to determine state. **Router and Switch are UP**—enquiries and status messages are going back and forth. **Router is UP, Switch is DOWN**—the router is sending enquiries, but the switch isn't responding to them. **Router is DOWN, Switch is UNKNOWN**—the router is not sending enquiries, and because spoofing is disabled, the switch has no chance to send status messages. **Router is DOWN, Switch is UP**—the router is not sending enquiries, but the switch is sending status messages in response to the DSU's spoofed enquiries. **Router and Switch are DOWN**—the router is not sending enquiries, and the switch is not sending status messages in response to the DSU's spoofed enquiries.
SPOOFING	This field indicates whether FRLM Polling Spoofing is occurring. Values are: **AS SERVICE**—DSU is acting as the switch and sending status responses back to the router. **AS CUSTOMER**—DSU is acting as the router and is sending enquiries to the switch. **INACTIVE**—DSU is not spoofing. **DISABLED**—Spoofing is disabled.
Spoofing Events: As Service=	The number of times the DSU went into spoof mode and acted as the service/switch (sends status messages back to customer/router).
Spoofing Events: As Customer=	The number of times the DSU went into spoof mode and acted as the customer/router (sends enquiry messages to the service/switch).
Spoofing Seconds: As Service=	The number of seconds the DSU was in spoof mode and acted as the service/switch (sends status messages back to customer/router).
Spoofing Seconds: As Customer=	The number of seconds the DSU was in spoof mode and acted as the customer/router (sends enquiry messages to the service/switch).
The next section contains data relating to the availability of VCs passing through the unit.	
DLCI	The Data Link Connection Identifier (DLCI) for which VC status is shown.
STATUS	Status of the VC as reported by the most recent status response message. Possible values are: **ACTIVE**—VC is active and ready to transport data **INACTIVE**—Switch knows about VC, but isn't ready to transport data over this VC. **NEW ACTIVE**—The switch has just created this VC, and it is active. **NEW INACTIVE**—The switch has just created this VC, and it is inactive. **NI TERM**—This VC is used only for communicating with the DSU from the switch, and the router has no knowledge of it. **DP TERM**—This VC is used only for communicating with the DSU from the router, and the switch has no knowledge of it. **NO COMM**—The router and switch are not communicating with each other using Link Management. Either the Switch is declared as DOWN, or the Router is DOWN and the DSU is not spoofing since spoofing is disabled. (In this case, the Switch can't send Status messages.)
ACTIVE SECONDS	The number of seconds the VC has been declared active by the FRLM status messages. Active Seconds do not increment when the switch is declared DOWN.
INACTIVE SECONDS	The number of seconds the VC has been declared inactive by the FRLM status messages. Inactive Seconds do not increment when the switch is declared DOWN.
# INACTIVE TRANSIT	The number of times the VC transitioned into the inactive state.

To display the report from the command line, use the following command:

VCAR[:*vc* [**Z**]]

vc	Enter the virtual circuit ID, a number from 1 to 1023, or * to view data for all VCs going through the unit.
Z	Clear the information in the report after displaying it. **Z** clears all the values and resets the “Start of Test” date and time.

Displaying and interpreting the VC Delay Report

*The **VCDR** report summarizes measured delays in the Frame Relay network for various VCs.*

The Virtual Circuit Delay Report (VCDR) command displays statistical counts for data gathered via Automatic Frame Relay PINGs (Auto-FPING). All measurements are from the perspective of the NI.

The following figure shows an example of a VC Delay Report.

```
KENTROX DataSMART 696 - VC Delay Report (Auto-FPING) - All VCs
NAME: PORTLAND, OR
Start of report:    Date: NOV 10, 1998    Time: 07:32
Current date/time:  Date: NOV 17, 1998    Time: 18:25
Report duration:       7 days 10 hrs 52 min 21 secs

       Auto-      ROUND-TRIP DELAY
 VC    Fping     Avg   Max   Total  Delay
DLCI   Status    msec  msec  Delay  Counts
----   -------   ----  ----  -----  ------
1004    WAIT     1234  1234  12345  123456
1004     UP      1234  1234  12345  123456
1004    DOWN     1234  1234  12345  123456
  35     UP        33    46     66       2
  45     UP        33    46     66       2
  46     UP        33    46     66       2
  55    WAIT        -     -      -       0
  65    DOWN       35    68    175       5
```

What to look for

- **Average delay meets expectations, or is not excessive**. You may wish to contact the carrier and ask what delay range they consider to be average. Remember the DataSMART FrameVision DSU measures round trip delay. The carrier may quote one-way delay which should be multiplied by 2 to get the equivalent delay as measured in the DataSMART 696/698.
- **The delay for some VCs is frequently above the threshold** you have set in the DataSMART FrameVision DSU. Either your threshold value is not within the typical delay range recommended by the carrier, or the Frame Relay service truly has delays above normal expectations. You may wish to select a particular VC and run an FPTST to get a real time feel for the actual Frame Relay delays. If excessive delays persist, consult with your carrier.
- **VCs where the auto-FPING status is down, not monitored.** If the VC has a DataSMART FrameVision DSU at the far end and you want to measure delays, you need to determine why FPING is not running and try to restart the FPING process manually.

Field header	Description
VC DLCI	The DLCI this data was gathered on.
Auto-FPING Status	**WAIT**—LMI has indicated that the VC is active. FPINGs have been sent but not received. **UP**—FPINGs are being sent and received. **DOWN**—LMI has indicated that the VC is inactive. Unit has stopped sending FPINGs.
These columns relate to delay measurements as gathered by background FPINGs.	
Avg	The average delay in msec for this VC as measured by Auto-FPING.
Max	The maximum delay in msec for this VC as measured by Auto-FPING.
Total Delay	The sum of all delay measurements made for this VC.
Delay Counts	The number of delay measurements made for this VC.

Displaying the report from the command line

Use the following command:

VCDR[:*vc* [**Z**]]

vc	Enter the virtual circuit ID, a number from 1 to 1023, or ***** to view data for all VCs going through the unit.
Z	Clear the information in the report after displaying it. **Z** clears all the values and resets the “Start of Test” date and time.

Displaying and interpreting the VC Frames Delivered Report

The VDFR report displays statistical counts for delivered frames and octets. This data is gathered via Auto-FPINGs.

The following figure shows an example of a VC Frames Delivered Report.

```
KENTROX DataSMART 696 - VC Frames Delivered Report (Auto-FPING) - All VCs
NAME: PORTLAND, OR
Start of report:    Date: NOV 10, 1998    Time: 07:32
Current date/time:  Date: NOV 17, 1998    Time: 18:25
Report duration:       7 days 10 hrs 52 min 21 secs

       Auto-       TX       RX       TX       RX
 VC    FPING     DROPPED  DROPPED  DROPPED  DROPPED
DLCI   Status    OCTETS   OCTETS   FRAMES   FRAMES
----   -------   -------  -------  -------  -------
1234    WAIT     1234567  1234567  1234567  1234567
1234     UP      1234567  1234567  1234567  1234567
1234    DOWN     1234567  1234567  1234567  1234567
  35     UP         5000    10000  1234567  1234567
  45     UP            -        -  1234567  1234567
  46     UP            -        -        -        -
  55    WAIT           -        -  1234567  1234567
  65    DOWN        5000     9000  1234567  1234567
```

Field header	Description
VC DLCI	The DLCI this data was gathered on.
The second column gives the current status of the Auto-FPING. The source for this status is the same as that for the VC Delay Report.	
Auto-FPING Status	**WAIT**—LMI has indicated that the VC is active. FPINGs have been sent but not received. **UP**—FPINGs are being sent and received. **DOWN**—LMI has indicated that the VC is inactive. Unit has stopped sending FPINGs.
The third group of columns relate to dropped frame measurements as gathered by background FPINGs. These statistics indicate whether the Frame Relay network is dropping user data frames at both ends of a VC.	
Tx Dropped Octets	Number of octets dropped in the transmit direction.
Rx Dropped Octets	Number of octets dropped in the receive direction.
Tx Dropped Frames	Number of frames dropped in the transmit direction.
Rx Dropped Frames	Number of frames dropped in the receive direction.

Displaying the report from the command line

Use the following command:

VDFR[:*vc* [**Z**]]

vc	Enter the virtual circuit ID, a number from 1 to 1023, or ***** to view data for all VCs going through the unit.
Z	Clear the information in the report after displaying it. **Z** clears all the values and resets the “Start of Test” date and time.

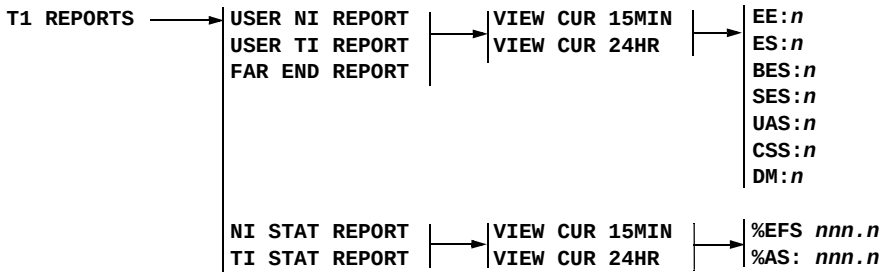
Accessing reports from the front panel

The front panel provides T1 performance reports for the network interface and the far end. It also provides a statistical version of the network interface data. The T1-layer information available from the front panel is limited to the current 15-minute interval and the current 24-hour interval.

Frame monitoring reports are also available from the front panel for the transmit and receive directions. These reports display information for the current 2-hour interval, the current 24-hour interval, and the current 15-minute interval.

Performance reports

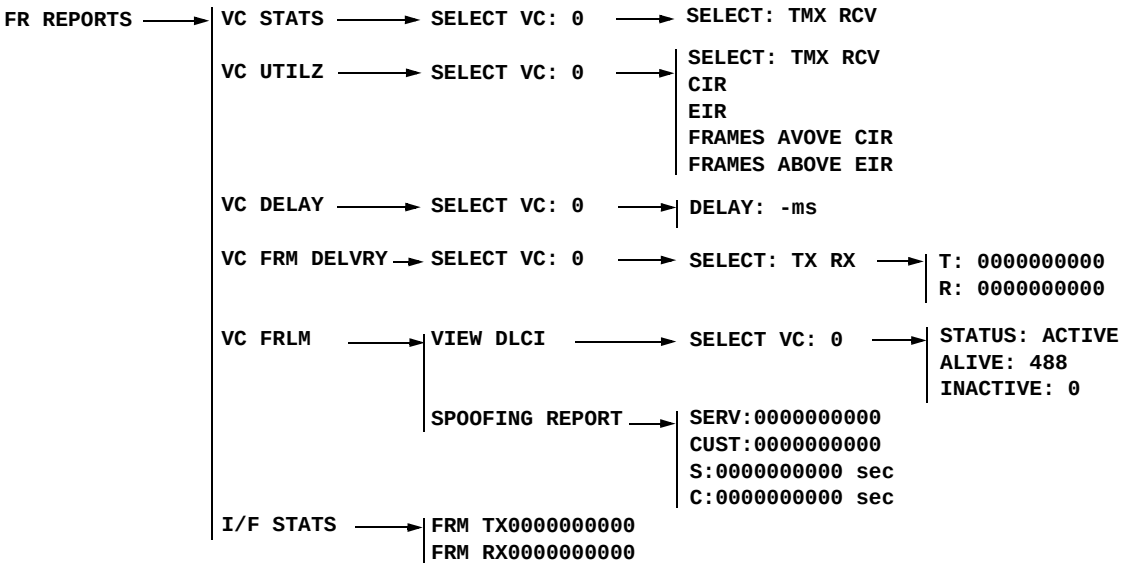
To view the performance reports from the front panel, use these steps.



1. When you see the desired report in the display, push Select. VIEW CUR 15MIN appears in the display.
2. Push Next or Previous to switch to VIEW CUR 24HR, if desired.
3. Push Select to view the first report display.
4. Push Next or Previous to cycle through the report displays.

Frame reports

To view the frame performance reports from the front panel, use these steps.



1 When you see the desired report in the display, push Select. VIEW CUR 15MIN appears in the display.

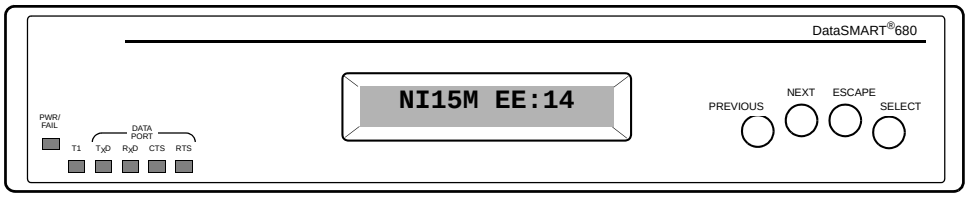
2 Push Next or Previous to switch to VIEW CUR 24HR, if desired.

3 Push Select to view the first report display.

4 Push Next or Previous to cycle through the report displays.

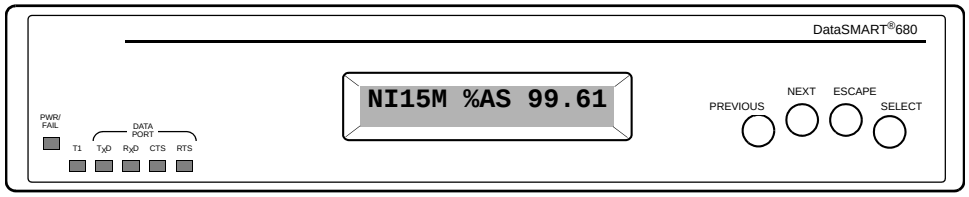
Interpreting the LCD performance display

The figure below shows a situation in which the user has selected the User NI Report for the current 15-minute time period, as indicated by “NI15M” in the display. The display is positioned at the count for error events. Pushing Next or Previous will cycle through displays to show the counts for errored seconds, bursty errored seconds, and others.



The display is dynamic. The counts in the display update as new events occur. If the display is for the current 15-minute interval, the count resets to zero when a new 15-minute interval is entered (at 00:15, 00:30, 00:45, etc.). If the report shows the current 24-hour interval, the interval is rolling and always shows the totalled count for the previous ninety-six 15-minute intervals.

The display for the statistical information is similar to the performance reports. For example, the figure below shows the User NI Report’s percentage of available seconds for the current 15-minute time period.



Clearing the performance database

At any time, you can clear the performance data and reset counters by executing the **ZERO COUNTERS** command under the **SYSTEM CFG** menu (see “Zeroing all counters” on page 39). This clears the data from all reports except the Alarm History and Security History reports.

Performance data is also cleared whenever you reset the date or time on the DataSMART using the **SET DATE** or **SET TIME** commands under the **SYSTEM CFG** menu (see “Setting date and time” on page 33).

C H A P T E R

9 Troubleshooting

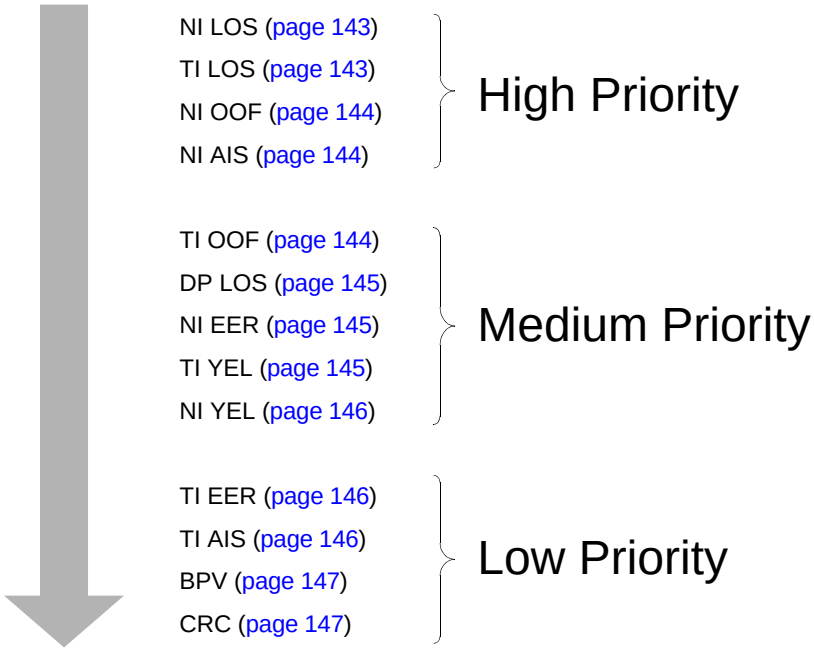
This chapter describes how to troubleshoot the DataSMART. It contains:

- How LEDs and alarm messages alert you when something is wrong
- How to find out the type of alarm and the interface at which it is occurring, using either the front-panel or the command-line interface
- A list of all error conditions in the System Status report and suggestions of how to resolve them
- A description of how to use the DataSMART diagnostic tools, including self test, loopbacks, and BERTs
- A description of how to use Frame PINGs (FPINGs) to troubleshoot frame connection problems

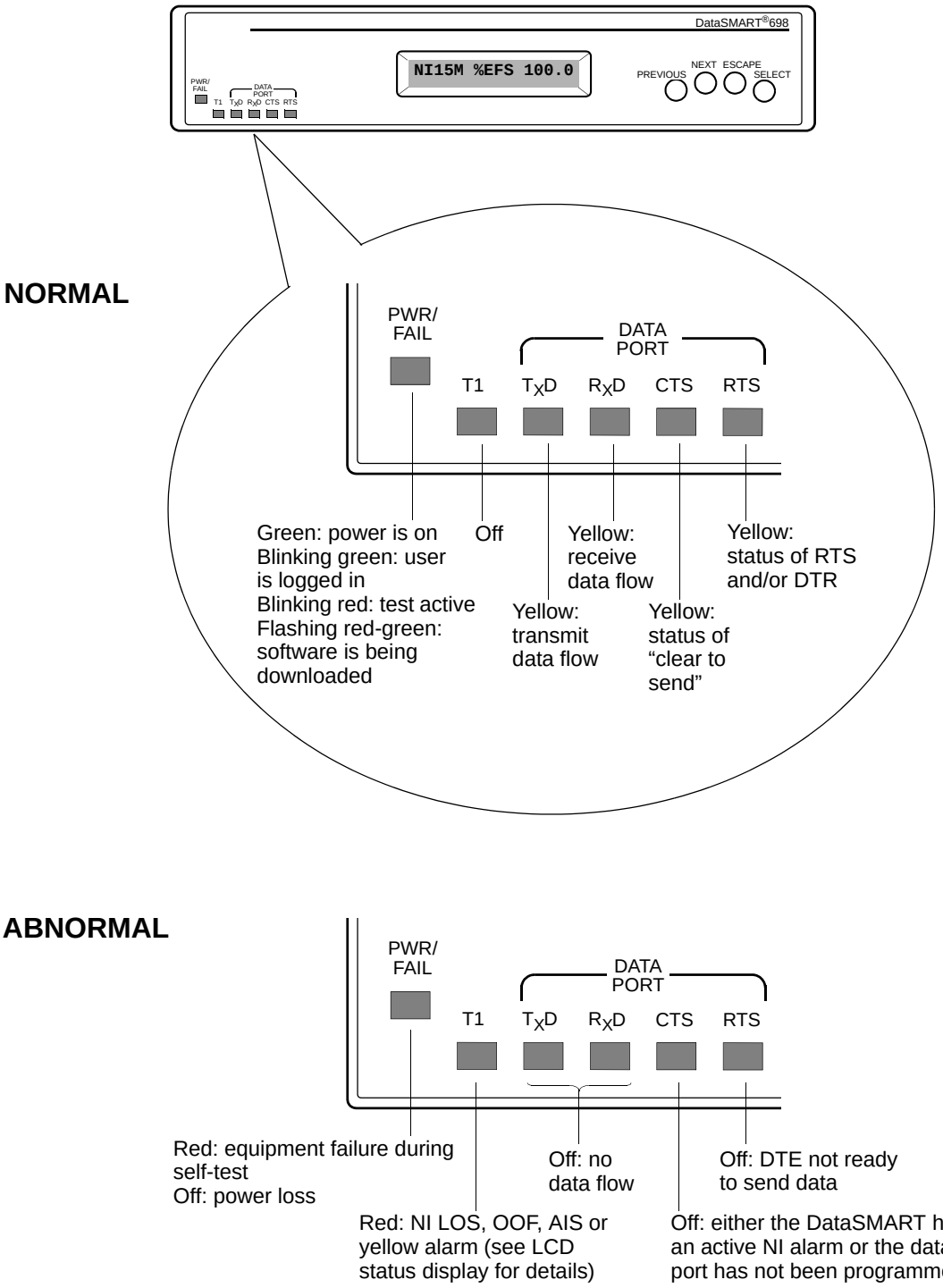
The pages in this chapter provide appropriate troubleshooting procedures for the alarms generated by the DataSMART. The alarms are prioritized high to low.

TIP
Always deal with the highest-priority alarms first.

Figure 14—Troubleshooting the DataSMART



Interpreting the front-panel LEDs



Monitoring alarm messages

Table 7—LED indicators and their meanings

LED	Indicator	Condition
PWR/FAIL	Green	Power is on, self-test successful.
	Green, blinking	A user is logged into the DataSMART.
	Red-to-green, flashing	Software program is being downloaded.
	Blinking red	A test is active.
	Red	Power is on, self-test failed.
	Off	No power is being received.
T1	Red	One or more of the following has occurred on the network interface or terminal interface or both (see LCD status display): ■ LOS alarm. The T1 signal has been lost. ■ OOF alarm. The T1 signal is out-of-frame. Some or all of the DS1 framing bits have been lost. ■ Incoming AIS alarm. The far-end equipment (NAIS) or CPE (TAIS) is in test or alarm state. ■ Yellow alarm. The far-end equipment (NYEL) or CPE (TYEL) is experiencing LOS or OOF.
TxD	Yellow	Data is being received from the DTE. Under normal conditions, this LED may fluctuate in intensity.
	Extended “off”	Flag characters (7E hex) are being received at the data port. Flags are transmitted to the network if RTS and CTS are high.
RxD	Yellow	Data is being transmitted to the DTE. Under normal conditions, this LED may fluctuate in intensity.
	Off	Flag characters (7E hex) are being output at the data port if RTS and CTS are on.
CTS	Yellow	Channels are assigned, and NI is not in alarm or in test mode. The DataSMART is ready to exchange data with the DTE.
	Off	This LED is off when it is not possible to transmit data out the data port. This may be because an NI alarm or test is present, or no channel is assigned to the data port.
RTS	Yellow	Request to send is asserted. The DTE is ready to send data to the DataSMART, according to the conditions established by the DPLOS command.
	Off	The DTE is not ready to send data (per the conditions configured by the DPLOS command), is not connected, or channels are not assigned.

The DataSMART generates the alarm messages listed in Table 8 and outputs them at the control port. If you receive an alarm message, you should use the Status (**S**) command to get the details of the problem.

Terminal interface alarms are generated by add/drop units only.

Only one alarm can be active at a time per unit. If two alarm conditions exist on a unit, that unit issues an alarm message only for the higher priority alarm. When the higher priority alarm is cleared, the unit then issues the next lower priority alarm, if one is still present.

Table 8—Alarms generated by DataSMART units

Alarm	Description
NI LOS	Loss of T1 signal at the network interface.
NI AIS	Incoming AIS (alarm indicator signal) at the network interface. Some device upstream of the network interface is in an OOF or LOS alarm state on the far side or in a test mode.
NI OOF	Out-of-frame T1 signal at the network interface. Some or all DS1 framing bits have been lost.
NI YEL	Incoming yellow alarm at the network interface. A device upstream of the network interface is in an OOF or LOS alarm state on the near side.
NI EER	Excessive error rate detected on the T1 signal at the network interface.
TI LOS	Loss of T1 signal at the terminal interface.
TI AIS	Incoming AIS (alarm indicator signal) at the terminal interface. Some device upstream of the terminal interface is in an OOF or LOS alarm state on the far side.
TI OOF	Out-of-frame T1 signal at the terminal interface. Some or all DS1 framing bits have been lost.
TI YEL	Incoming yellow alarm at the terminal interface. A device upstream of the terminal interface is in an OOF or LOS alarm state on the near side.
TI EER	Excessive error rate detected on the T1 signal at the terminal interface.
DP LOS	Loss of DTR and/or RTS at the data port.

Examining system status

If the DataSMART is in an alarm state or if you notice an abnormal condition, use the System Status report display to get more information. You can view the system status from the front-panel or the command-line interface. Both the front-panel display and the command-line report use the same status codes, which are explained in Table 9 on page 140.

Terminal interface alarms are generated only by add/drop units.

TIP
For a discussion of how the DataSMART transitions in and out of alarm states based on errored signal conditions, see "T1 alarms and signal processing" on page 177 .

The system status tells you the current condition of the DataSMART, including any alarms that may be active as well as current—and possibly intermittent—signal conditions at the network interface, the terminal interface, and the data ports. Both the LCD status display and the command-line status display are dynamic and are updated as conditions change on the DataSMART.

Using the command line

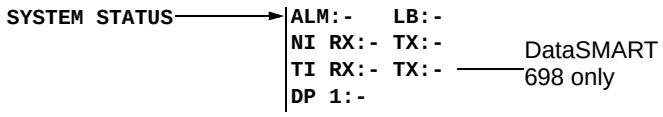
To see the command-line display, enter **S** at the prompt. A screen similar to the one shown below appears. The display is updated once per second if the status changes, with the new status line added at the bottom. You exit the display by pressing Ctrl-C.

```
OPERATIONAL STATUS (^C TO EXIT)

DEC  4, 1998

TIME   SYSTEM     NI       TI       Data Port
-----  ---------  -------  -------  ---------
       ALRM LPBK  IN  OUT  IN  OUT  DP1
-----  ---- ----  --- ---  --- ---  ---
07:31  NLOS -     LOS YEL  LOS AIS  CON
```

Screen column	Description
TIME	This column shows the time of day (in 24-hour format) that the status line was generated.
SYSTEM ALRM	This column shows the highest priority state.
SYSTEM LPBK	This column shows if a loopback is active.
NI IN, NI OUT	These columns show the network interface receive and transmit signal conditions.
TI IN, TI OUT	These columns show the terminal interface receive and transmit signal condition (add/drop units only).
Data Port	This column shows the data port input signal condition.

Using the front panel

To view system status from the front panel:



Status codes

Table 9 explains the status codes and provides a page reference for possible solutions.

Table 9—Status codes

Code	Description	Solution
ALM—Alarm Status		
—	No alarm exists.	Normal behavior.
NLOS	Loss of the network input signal.	See page 143.
NOOF	The network input signal is out of frame.	See page 144.
NAIS	Incoming AIS (alarm indication signal) at the network interface.	See page 144.
NYEL	Incoming yellow alarm at the network interface.	See page 146.
NEER	Excessive error rate detected on the network input signal.	See page 145.
TLOS	Loss of the terminal input signal.	See page 143.
TOOF	The terminal input signal is out of frame.	See page 144.
TAIS	Incoming AIS (alarm indication signal) at the terminal interface.	See page 146.
TYEL	Incoming yellow alarm at the terminal interface.	See page 145.
TEER	Excessive error rate detected on the terminal input signal.	See page 146.
1LOS	Loss of DTR and/or RTS at data port 1.	See page 145.
LB—Loopback Status		
—	No loopback is set.	Normal behavior.
RLLB	Code has been sent to set a remote line loopback.	Loopback test in progress.
RPLB	Code has been sent to set a remote payload loopback.	Loopback test in progress.
RDP1	Code has been sent to set remote data port loopback.	Loopback test in progress.
LLB	A line loopback is set on the local device.	Loopback test in progress.
LOC	A local loopback is set on the local device.	Loopback test in progress.
PLB	A payload loopback is set on the local device.	Loopback test in progress.
TLB	A terminal loopback is set on the local device.	Loopback test in progress.
DP1	A data port loopback is set on the local device.	Loopback test in progress.
DT1	A data terminal loopback is set on the local device.	Loopback test in progress.
NI Rx—Network Input Status		
LOS	Loss of the network input signal.	See page 143.
OOF	The network input signal is out of frame.	See page 144.
AIS	Incoming AIS (alarm indication signal) at the network interface.	See page 144.
YEL	Incoming yellow alarm at the network interface.	See page 146.

Table 9—Status codes (continued)

Code	Description	Solution
BPV	A bipolar violation has been detected on the network input signal. This applies only if the network signal is using SF framing.	See page 147.
QRS	A BERT running QRS test code is active at the network interface.	Normal behavior when a BERT is active.
324	A BERT running 3 in 24 test code is active at the network interface.	Normal behavior when a BERT is active.
247	A BERT running 2047 test code is active at the network interface.	Normal behavior when a BERT is active.
511	A BERT running 511 test code is active at the network interface.	Normal behavior when a BERT is active.
1’S	A BERT running all 1s test code is active at the network interface.	Normal behavior when a BERT is active.
0’S	A BERT running all 0s test code is active at the network interface.	Normal behavior when a BERT is active.
—	Valid data is being received. No errors detected.	Normal behavior.
NI Tx—Network Output Status		
AIS	AIS (alarm indication signal) is being transmitted out the network interface.	See page 144.
YEL	Yellow alarm is being transmitted out the network interface. This occurs when LOS, OOF, or incoming AIS is detected at the network input signal.	See the entry in this table for Network input status codes LOS, OOF, or AIS.
QRS	QRS test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
324	3 in 24 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
247	2047 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
511	511 test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
1’S	All 1s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
0’S	All 0s test code is being transmitted out the network interface.	Normal behavior when a BERT is active.
COD	The DataSMART is in the process of setting or resetting a remote loopback.	Normal behavior.
—	Valid data is being transmitted out the network interface.	Normal behavior.

Table 9—Status codes (continued)

Code	Description	Solution
DP1—Data Port Status		
—	No bandwidth (channels) have been assigned to the data port.	Normal behavior.
CON	Bandwidth is assigned to the port, and the port is not in a LOS condition.	Normal behavior.
LOS	Bandwidth is assigned to the port, but a loss of DTR or RTS has been detected.	See page 145.
TI Rx—Terminal Input Status (698 only)		
LOS	Loss of the terminal input signal.	See page 143.
OOF	The terminal input signal is out of frame.	See page 144.
AIS	Incoming AIS (alarm indication signal) at the terminal interface.	See page 146.
YEL	Incoming yellow alarm at the terminal interface.	See page 145.
BPV	A bipolar violation has been detected on the terminal input signal.	See page 147.
—	Valid data is being received. No errors detected.	Normal behavior.
TI Tx—Terminal Output Status (698 only)		
YEL	Yellow alarm is being transmitted out the terminal interface. This occurs when incoming yellow alarm is detected at the network input signal.	Troubleshoot the alarm causing the output.
AIS	AIS (alarm indication signal) is being transmitted out the terminal interface. This occurs when LOS, OOF or incoming AIS is detected on the network input signal.	Troubleshoot the alarm causing the output.
—	Valid data is being transmitted out the terminal interface.	Normal behavior.

Troubleshooting tree

Troubleshooting alarms

The best troubleshooting method is to start with the highest priority alarm, find its cause and fix it, and then turn to the next highest priority. The following alarm list is arranged from high to low priority. You may also want to use some of the diagnostic tools described later in this chapter.

NOTE
In this manual, high-priority alarms tend to arise from more basic problems than low-priority alarms. Often, fixing a high-priority alarm will also automatically correct alarms of lower priority. Network management systems use the words "critical," "major," and "minor" to rank alarms in terms of seriousness. These two rankings are similar, but not always identical.

NI LOS—high priority

If you receive a loss-of-signal condition at the network interface

An NI LOS condition occurs when the DataSMART cannot detect a signal at its network interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART network interface and your T1 service provider's equipment.
- If you built the cable on-site, check the cable connectors. A reversal of the transmit and receive pairs, or an open receive pair, can cause this condition.
- If the above appear to be okay, ask your T1 service provider to test your T1 line and correct any problems found.

TI LOS—high priority

If you receive a loss-of-signal condition at the terminal interface

A TI LOS condition occurs when the DataSMART cannot detect a signal at its terminal interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART terminal interface/data port and your CPE equipment.
- If you built the cable on-site, recheck the cable connectors. A reversal of the transmit and receive pairs, or an open transmit pair (CPE-to-DataSMART), can cause this condition.

NOTE
If you assign channels to the terminal interface but do not connect equipment to it, the unit will generate the TI LOS alarm.

NI OOF—high priority

If the incoming signal at the network interface is out-of-frame

An out-of-frame condition occurs when the framing type you have configured for the network interface does not match the framing type of the incoming T1 signal. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the network interface (see "Specifying NI framing format" on page 53), or
- Ask your T1 service provider to change the framing type of your T1 line.

A highly-errored incoming signal can also cause an OOF condition.

NI AIS—high priority

If an alarm indication signal (AIS) is detected at the network interface

An incoming AIS at the network interface indicates a problem with remote equipment on the T1 circuit. For example, the far-end equipment may not be connected or configured properly or is in a test mode, or the network interface unit (i.e., NIU or smart jack) may be in loopback, or your service provider may not have enabled your circuit yet. To troubleshoot this condition:

- Ask your T1 service provider to trace the source of the AIS signal.

TI OOF—medium priority

If the incoming signal at the terminal interface is out-of-frame

An out-of-frame condition occurs when the framing type you have configured for the terminal interface does not match the framing type of the signal being received at the terminal interface. Allowed framing types are ESF, SF, or Ericsson. To troubleshoot this condition:

- Change the framing type of the terminal interface (see "Specifying NI framing format" on page 53), or
- Change the framing type of the attached CPE equipment.

A highly-errored incoming signal can also cause an OOF condition. Check the description of TI EER.

DP LOS—medium priority

If you receive a loss-of-signal indication at the data port

A DP LOS condition occurs when the DataSMART is not able to handshake as expected with an attached DTE device.

The DataSMART can monitor two handshake lines on each data port: DTR and RTS. You can configure your DataSMART to use either, or both lines as the DP LOS criteria (see "Setting up DP LOS (data port loss of signal) processing" on page 64). When the specified line goes low, the DataSMART assumes that the DTE equipment has been disconnected or has failed. To troubleshoot this condition:

- Check the cable connection between the DataSMART data port and the DTE.
- Verify that the cable is connected to the correct port at each end.
- Verify that you are using the correct cable for your application.
- Make sure that the DTE is powered up and that its serial port is activated.

Refer to the DataSMART 696/698 Installation Guide for instructions on how to properly connect cables.

NI EER—medium priority

If an excessive error rate is detected at the network interface

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the network interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting (see page 47).
- Make sure that you have correctly connected the cable between the DataSMART network interface and your T1 service provider's equipment. (Refer to the DataSMART 696/698 Installation Guide for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the network interface to match the line coding of your T1 line: either AMI or B8ZS. (See "Specifying NI line coding" on page 54.)
- Make sure the system clock is configured correctly.
- If all the above appear to be okay, ask your T1 service provider to test your T1 line and correct any problems found.

TI YEL—medium priority

If incoming yellow alarm is detected at the terminal interface

An incoming yellow alarm at the terminal interface indicates that the CPE equipment attached to the interface is having a problem with the signal it is receiving from the DataSMART. Most often, it is getting no signal at all. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART terminal interface port and the CPE equipment. An open receive pair (DataSMART TI port output to CPE input) can cause this condition.

NI YEL—medium priority

If incoming yellow is detected at the network interface

An incoming yellow condition at the network interface indicates that the far end equipment has a problem with the signal it is receiving from the DataSMART. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART network interface port and your T1 service provider's network interface unit (i.e., NIU or smart jack). An open transmit pair can cause this condition.
- If your application uses SF framing, and all 24 channels are used for data transmission, the actual data content can sometimes cause a "false yellow" condition. ESF framing is recommended for such applications. Other work-arounds may also be possible, depending upon your application.

TI EER—low priority

If an excessive error rate is detected at the terminal interface

The errors may be BPVs, CRC6 errors, or framing errors. There are several potential causes of an excessive error rate at the terminal interface. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting.
- Make sure that you have correctly connected the cable between the DataSMART terminal interface/data port and your CPE equipment. (Refer to *DataSMART 696/698 Installation Guide* for instructions on how to properly connect the cable.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure that you have configured the line coding of the terminal interface to match the line coding of your CPE equipment: either AMI or B8ZS. (See "Specifying TI line coding" on page 58.)
- Make sure the system clock is configured correctly.

TI AIS—low priority

If an alarm indication signal (AIS) is detected at the terminal interface

An incoming AIS at the terminal interface may indicate that the CPE equipment attached to the terminal interface is not operational. To troubleshoot this condition:

- Check the programming of the CPE and make sure that its TI port is enabled.
- Check the wiring between the DataSMART TI port and the CPE.
- Make sure that the framing type of the CPE matches the framing type configured for the terminal interface. Allowed framing types are ESF, SF, and Ericsson. (See "Specifying TI framing format" on page 58.)

BPV—low priority

If bipolar violations (BPVs) are detected at the network interface or the terminal interface

A bipolar violation is an error in the normal polarity of received pulses. A bipolar violation occurs when two or more pulses of the same polarity appear in a row.

Bipolar violations are often caused by local problems with your T1 line. To troubleshoot this condition:

- Make sure that your T1 wiring consists of only *individually-shielded* twisted pairs.
- Check that all cable connections are secure and connected to the correct terminals. Refer to the DataSMART 696/698 Installation Guide for instructions on how to properly connect cables.
- Make sure that you've set the line coding of the network interface to match the line coding of the T1 circuit: either AMI or B8ZS. A mismatch in line coding can often result in BPV errors.
- Make sure the system clock is configured correctly.

CRC—low priority

If CRC6 (6-bit cyclic redundancy check) errors are detected at the network interface or the terminal interface

CRC6 errors relate to ESF framing only. A CRC6 error indicates that bits were received in error in the previous extended superframe.

CRC6 errors are often caused by remote problems with your T1 line. To troubleshoot these types of errors:

- Make sure that you've set the line coding of the network interface to match the line coding of the T1 circuit: either AMI or B8ZS. This line code should be maintained throughout the connected circuit. A mismatch in line coding can often result in CRC6 errors.
- If the errors show up on the NI port, ask your T1 service provider to monitor the receive side of your line for CRC6 errors.
- Make sure the system clock is configured correctly.

Running the self-test diagnostics

At any time, you can initiate the DataSMART self-test. The self-test verifies the functions of DataSMART hardware circuitry. There will be a brief service interruption during the self-test.

When you execute the self-test, the DataSMART automatically resets any loopbacks. It does not clear the performance database, nor does it log you out of the system.

You cannot activate the self-test if you have logged into the DataSMART remotely through Telnet or SNMP. The self-test would break your remote login connection.

Using the command line

To initiate self-test from the command line, enter the **DST** command. You must have super-user, configuration, or maintenance privileges.

Using the front panel

To initiate self-test from the front panel:

LOCAL MAINT → **DO SELF TEST** → **DO SELF TEST ?**

Push Select to start the self-test or Escape to abort.

Self-test error messages

The following messages announce pass or fail conditions discovered by the self-test. Contact our Technical Support organization if the self-test returns a “fail” condition.

Command-line display	Front-panel display
RESET TEST MODES FIRST	RESET TEST MODES
SELF TEST PASSED	SELF TEST PASSED
UNABLE TO PERFORM SELF TEST	UNABLE TO TEST
FLASH TYPE FAIL	FLASH TYPE FAIL
FLASH PROGRAM WORD FAIL	FLASH WORD FAIL
FLASH PROGRAM CHECK SUM FAIL	FLASH SUM FAIL
RTC TEST FAILED	RTC TEST FAILED
NI READ/WRITE TEST FAILED	NI R/W TEST FAIL
TI READ/WRITE TEST FAILED	TI R/W TEST FAIL
CGD DETECTION TEST FAILED	CGD DETECT FAIL
CGD BIT ERROR RATE TEST FAILED	CGD DATA FAIL

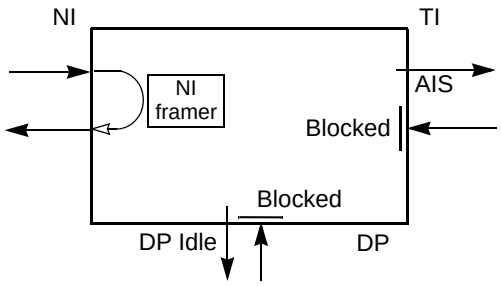
Using loopbacks

The DataSMART provides loopbacks to support line segment testing. Line segment testing allows you to probe the T1 circuit to isolate where data flow is being corrupted or disrupted.

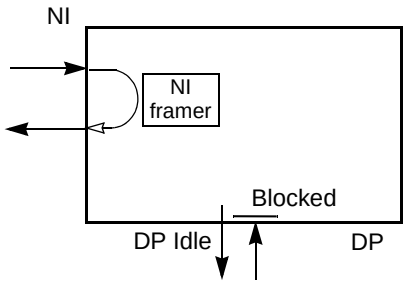
You can set all loopbacks locally, in your near-end device. You can also set the line, payload, and data port loopbacks remotely, in a far-end device.

Line loopback

Add/Drop



DSU



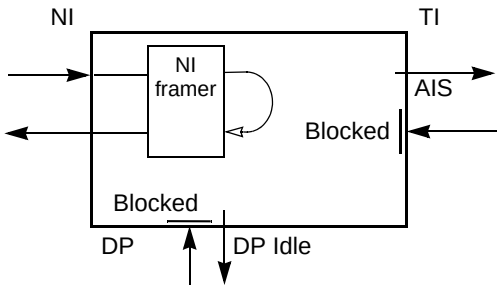
The line loopback allows the carrier (or a far-end device) to test the T1 signal at the DataSMART network interface. When set to line loopback, the DataSMART loops the incoming T1 signal back to the network. The T1 signal does not penetrate the DataSMART (it is a minimum-penetration loopback), and does not pass through the DataSMART framer. The signal, including framing and line coding errors, is returned to the network unaltered and the carrier can test the looped signal for errors.

Once the line loopback is set, the incoming network signal is interrupted, so the DataSMART outputs AIS at the terminal interface and idle characters at the data port.

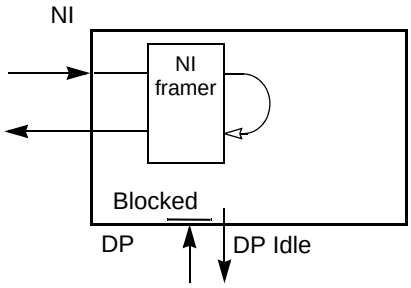
You can set the line loopback locally using the command line or front panel (see page 155); or remotely in a far-end device (see page 157).

Payload loopback

Add/Drop



DSU



By testing the T1 signal through a line loopback as described earlier, the carrier (or the far-end device) can determine if there are problems in the network line. What they cannot determine, however, is whether the problems are occurring on the input or output side of the looped line. To further isolate the source of the problems to one side of the line or the other, you can change from a line loopback to a payload loopback.

Payload loopback is the same as line loopback, except that the signal passes through the DataSMART framer before being looped back. The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

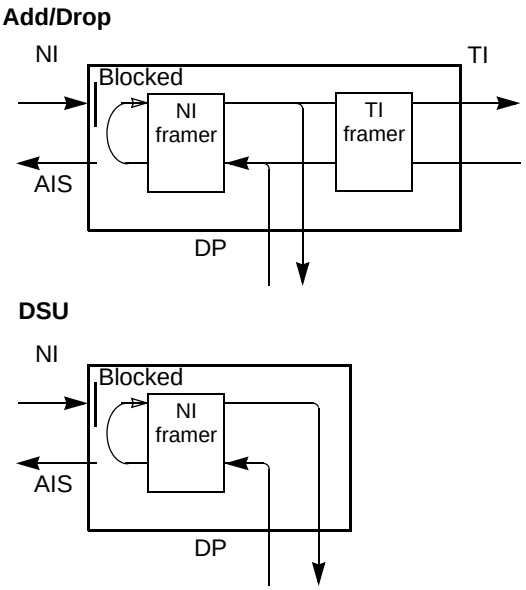
The condition of the returned signal indicates the cause of the problem:

- The line is okay if the returned signal contains no bit pattern errors, no BPVs, and no CRC6 errors.
- The problem is outbound if the returned signal contains pattern bit errors, but no BPVs or CRC6 errors.
- The problem is inbound and at the remote end if the returned signal contains pattern bit errors and CRC6 errors, but no BPVs.
- The problem is inbound and at the local end if the returned signal contains pattern bit errors, CRC6 errors, and BPVs.
- The problem is probably a remote clock slip if the returned signal contains pattern bit errors and is bursty, but contains no BPVs and no CRC6 errors.

Once the payload loopback is set, the incoming network signal is interrupted, and so the DataSMART outputs idle characters at the data ports and AIS at the terminal interface.

You can set the payload loopback locally at the request of the carrier or a far-end site (see page 155), or you can set it remotely in a far-end device (see page 157).

Local loopback



TIP
The local loopback is similar to a "hard" loopback set at the network interface.

Add/Drop units

The local loopback allows you to verify if the DataSMART is assigning channels correctly to the terminal interface and data port. When set in this loopback, the DataSMART combines all the incoming channels from the terminal interface and data port into the T1 bit stream, runs the bit stream through the NI framer, loops the bit stream back, and drops out the channels to the data port and/or terminal interface. By attaching terminal devices capable of monitoring the looped signals, you can verify that the correct channels are being returned to the correct ports.

DSUs without terminal interface

The local loopback allows you to test transmission from the DTE to the data port. This loopback combines all the incoming channels from the data port into the T1 bit stream, runs the bit stream through the NI framer, loops the bit stream back, and returns the assigned channels to the data port. By attaching a DTE device capable of monitoring the looped signal, you can verify the quality of the returned signal.

All units

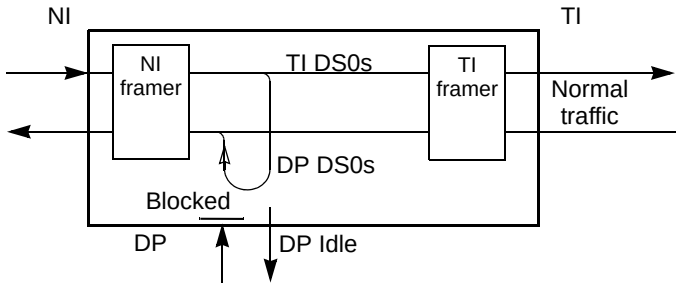
When the DataSMART is set in a local loopback, the outgoing T1 signal at the network interface is interrupted. The DataSMART outputs AIS at the network interface.

The framer strips out BPV errors and recalculates CRC (for ESF framing format) but does not alter the payload data.

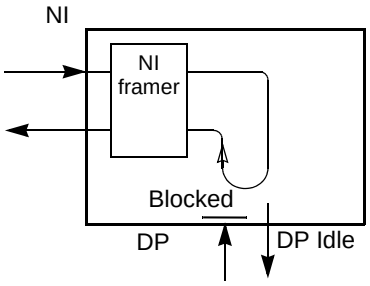
You can set a local loopback only in your local DataSMART (see page 155); you cannot set it remotely.

Data port loopback

Add/Drop



DSU



The data port loopback allows the carrier (or a far-end device) to examine the fractional DS0 channels assigned to the data port. When set to data port loopback, the DataSMART receives the T1 signal at the network interface, distributes the fractional DS0 channels as assigned to the data port, then loops the channels back to the network. It does this without affecting the rest of the received payload. Normal transmission occurs at the terminal interface.

Add/Drop units

Full-bandwidth test codes (QRS, 3 in 24, all 1s, all 0s) will fail if the unit has some network interface channels set to the terminal interface and others set to the data port because of differences in timing delays between the terminal interface and data port circuits. You can remedy this problem by doing one of the following during the test:

- Assign all channels to the terminal interface.
- Assign all channels to the data port (rate=64 kbps per channel).
- Use a different test pattern.

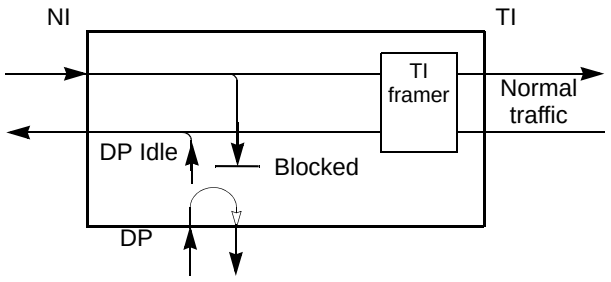
All units

Once the data port loopback is set, transmission at the data port is interrupted. The DataSMART sends idle characters out the port to notify the connected DTE device.

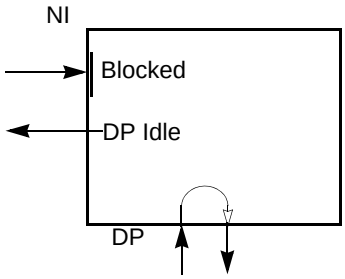
You can set the data port loopback locally to facilitate testing with the carrier or a far-end site (see page 155), or you can set it remotely in a far-end device (see page 157).

Data terminal loopback

Add/Drop



DSU



Typically, you use the data terminal loopback to verify the cabling between the data port and the attached DTE device. You can also monitor the looped signal for errors at the DTE.

The data terminal loopback allows you to loop the incoming signal at the data port. When set in this loopback, the DataSMART loops the incoming signal back to the DTE device sending the signal. The signal does not penetrate the DataSMART. The signal, including all line coding errors, is returned to the DTE device unaltered.

You can set a data terminal loopback only in your local DataSMART (see page 155); you cannot set it remotely.

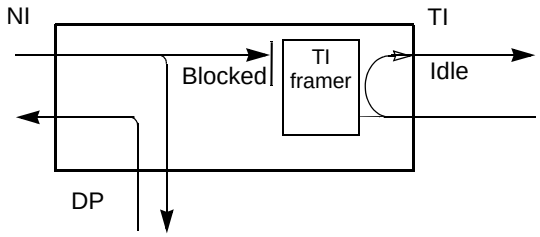
Add/Drop units

When set in a data terminal loopback, the DataSMART inserts the data port idle character into the channels assigned to the data port. Normal activity continues at the network interface and the terminal interface.

DSUs without terminal interface

When set in a data terminal loopback, the DataSMART outputs AIS or a framed all-ones signal at the network interface (see “Specify the “keep alive” signal for the network interface (add/drop units only)” on page 55).

Terminal interface loopback (add/drop units only)



Typically, you use the terminal interface loopback to verify the cabling between the terminal interface and the CPE. You can also attach a test set to the terminal interface, send test codes, then run bit error rate tests (BERTs) on the looped signal.

The terminal interface loopback allows you to loop the incoming T1 signal at the terminal interface in add/drop devices. When set in this loopback, the DataSMART loops the incoming T1 signal back to the CPE attached to the terminal interface. The signal does not penetrate the DataSMART. The signal, including all line coding errors, is returned to the CPE unaltered.

When set in a terminal interface loopback, the DataSMART inserts the TI idle character into channels assigned to the terminal interface. Normal activity continues at the network interface and data port.

You can set a terminal interface loopback only in your local DataSMART (see page 155); you cannot set it in a remote device.

Setting and resetting loopbacks in your local device

You can set and reset loopbacks in your local device from the command line. Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active.

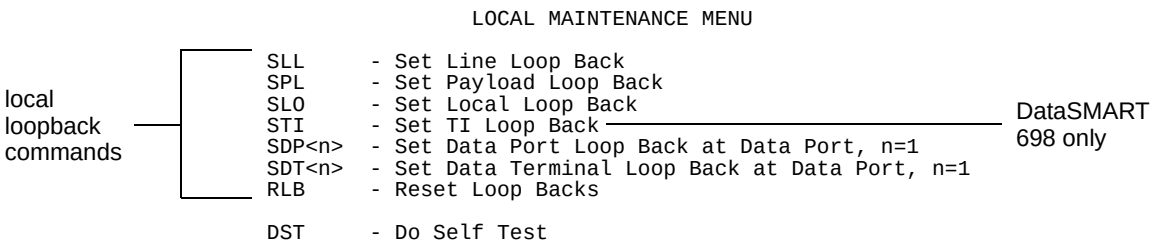
The DataSMART also allows you to set the line, payload, and data port loopbacks via Telnet or SNMP.

NOTE

A far-end device can set your local device in line, payload, or data port loopback by sending the remote loopback commands described in the next section. A far-end device can also set your device in line loopback by sending standard line loopback set and reset code, or in data port loopback by sending 127 set code and inverted 127 reset code (V.54 loop code).

Using the command line

The figure below illustrates the Local Maintenance menu. You use the commands in this menu to set or reset loopbacks in your local device. You must have super-user, configuration, or maintenance privileges.

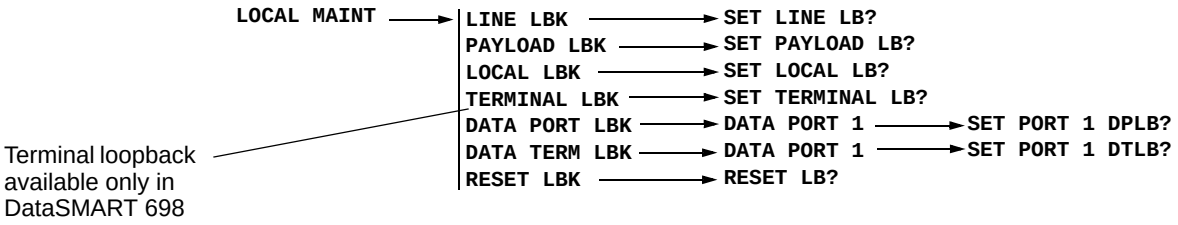


SLL	Set a line loopback.
SPL	Set a payload loopback.
SLO	Set a local loopback.
STI	Set a terminal interface loopback (in add/drop units only).
SDP1	Set a data port loopback on data port 1.
SDT1	Set a data terminal loopback on data port 1.

To reset a loopback in your local DataSMART, enter **RLB**.

Using the front panel

To set or reset local loopbacks from the front panel, use these steps. You must have super-user, configuration, or maintenance privileges.



1. From the LOCAL MAINT menu, push Next or Previous until the desired command appears in the display. The RESET LBK command is available only if a loopback has already been set.

2. Push Select. If you select either the data port loopback or the data terminal loopback, you must push Select for data port 1, then push Select again for the next command.

3. A query asks if you really want to set or reset the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.

4. After a few seconds, the message RESET LBK appears (“resetting” the loopback turns it off). When you are ready to turn the loopback off, push Select. A query asks if you really want to reset the loopback. Push Select to turn off the loopback.

Setting and resetting loopbacks remotely

You can set a line, payload, or data port loopback remotely, in a far-end device. If you set one of these loopbacks, you can then send a test code through the loop and run BERTs on the code to troubleshoot for errors. This section describes how to set and reset remote loopbacks. For a description of how to set and run test codes and BERTs, see page 159.

Only one loopback, either local or remote, may be set at one time. You cannot set a loopback if another loopback is already active, if a test code is being transmitted, or if a BERT is active. You cannot use the **SRL**, **SRP**, or **SRDP** commands in-band.

The figure below shows the Remote Maintenance menu. You use the commands listed in this menu to set and reset remote loopbacks. You must have super-user, configuration, or maintenance privileges.

Remote loopback commands

```
                    REMOTE MAINTENANCE MENU

SRL                 - Set Remote Line Loop Back
SRP                 - Set Remote Payload Loop Back
SRDP<n>             - Set Remote Data Port Loop Back, n = 1
RST1                - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1, 0
S5C<n>          - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>          - Send 2047 Test Code in Data Port <n> Bit Stream
RTC             - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1, 0
BT5<n>          - Activate BERT using 511 at Data Port n = 1
BT2<n>          - Activate BERT using 2047 at Data Port n = 1
```

SRL Set a remote line loopback.

SRP Set a remote payload loopback.

SRDP1 Set a remote data port loopback on data port 1.

To reset a remote loopback, enter **RST1**.

You may receive one or more of the following messages when setting or resetting remote loopbacks.

SENDING LOOP BACK SET CODE—The DataSMART is requesting a loopback.

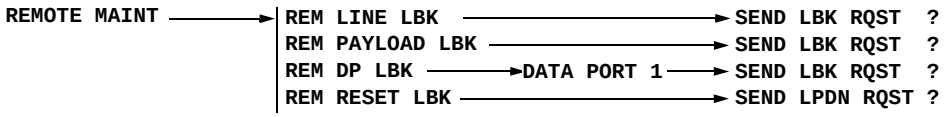
REMOTE LOOP BACK IS SET—The remote loopback is set.

UNABLE TO CONFIRM REMOTE LOOP BACK IS SET—The DataSMART tried to set the remote loopback but was unable to confirm that the loopback was set.

UNABLE TO SET REMOTE LOOP BACK—The DataSMART cannot set a loopback because a loopback is already set, a test code is being generated, or a BERT is active.

Using the front panel

To set remote loopbacks from the front panel:



1 When the desired loopback appears in the display, push Select. A query asks if you really want to set the loopback. Push Select to set the loopback. LOOPBACK SET appears in the display.

2 If you select the remote data port loopback, push Select for data port 1, then push Select again for the next command.

3 If you want to reset a remote loopback (turn the loopback off), push Select when REM RESET LBK appears in the display. You will be asked to verify this selection. Push Select again.

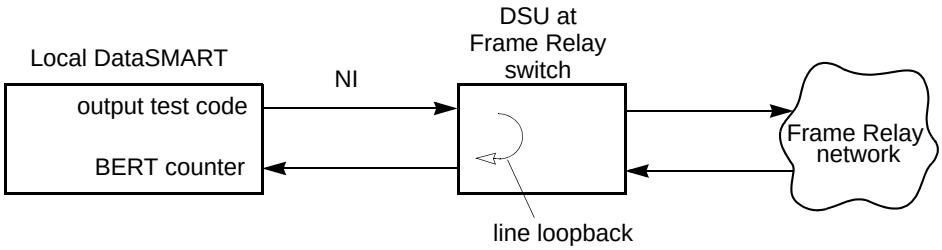
When you send a request to set or reset a loopback, you will receive one of several responses:

SENDING RQST	The DataSMART is in the process of sending the request.
NO CONFIRMATION	The DataSMART sent the request, but was unable to confirm that the loopback was set or reset.
LPBK CONFIRMED	The DataSMART sent the request and the loopback was confirmed as set or reset.
UNABLE TO SEND	The DataSMART is unable to send the request because a loopback is already set.

Using test codes and BERTs

BERTs in a Frame Relay network

You can use a bit error rate test (BERT) to test the T1-layer connection to your network. Although a BERT will not test Frame-level performance, you can use it to check the T1 link to the closest device in the Frame Relay network. A BERT allows you to send a test code through a looped-back line, then counts the errors returned in the signal. For example, the figure below illustrates how you might use a BERT in conjunction with a line loopback.



To use a BERT in conjunction with a remote loopback, do the following:

1. Set a hard loopback on the remote device. You can set a remote line or payload loopback to test the full T1 signal. On Kentrox DSUs, you can set a data port loopback to test the channels assigned to the data port.
2. Send test codes through the loop. To test the full T1 signal, send one of the following test codes: QRS, 3 in 24, all 1s, or all 0s.

   To test the channels assigned to the data port, send one of the following codes on those channels: 511 or 2047.
3. Activate the BERT and monitor the BERT error report.
4. Exit BERT.
5. Reset the test codes.
6. Reset the loopback.

How BERTs work

When a BERT is first activated, the DataSMART initializes all counters to zero. It starts monitoring the incoming network signal for the specified test pattern. (In the case of a data port loopback, the DataSMART looks for the specified test pattern only on the channels mapped to the specified data port.)

When the DataSMART recognizes the test pattern, it begins tracking time and errors. The time counter continues to count even during time of sync loss. The time and error counters continue to count until they reach their maximum limit as specified below; they do not roll over.

You can exit a BERT by typing Ctrl-C.

```
RM> btq
^C to TERMINATE
SEARCHING FOR PATTERN
Pattern Detected
   TEST      BIT  ERRORED   BURSTY  SEV ERR  UNAVAIL   TOTAL BIT
SECONDS  ERRORS  SECONDS  SECONDS  SECONDS  SECONDS      ERRORS
-------  ------  -------  -------  -------  -------   ---------
      1       0        0        0        0        0           0
      2       0        0        0        0        0           0
      3       0        0        0        0        0           0
      4       0        0        0        0        0           0
      5       0        0        0        0        0           0
      6       0        0        0        0        0           0
      7       0        0        0        0        0           0
      8       1        1        0        0        0           1
      9       3        2        1        0        0           4
     10       5        3        2        0        0           9
     11       6        4        3        0        0          15
     12       5        5        4        0        0          20
     13       5        6        5        0        0          25
     14       5        7        6        0        0          30
     15       4        8        7        0        0          34
     16       0        8        7        0        0          34
     17       0        8        7        0        0          34
     18       0        8        7        0        0          34
     19       0        8        7        0        0          34
     20       0        8        7        0        0          34
```

Field	Description
TEST SECONDS	The number of seconds, up to 2^{32} maximum, that the DataSMART has been running the test after first detecting the test pattern.
BIT ERRORS	The number of bit errors, up to 65,535 maximum, that have occurred in the current second.
ERRORED SECONDS	The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
BURSTY SECONDS	The number of bursty errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
SEV ERR SECONDS	The number of severely errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
UNAVAIL SECONDS	The number of unavailable seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.
TOTAL BIT ERRORS	The running total of bit errors, up to 2^{32} maximum, that have occurred since the DataSMART first detected the test pattern.

Command-line access

You set and reset test codes and activate a BERT by using the commands listed in the Remote Maintenance menu. You must have super-user, configuration, or maintenance privileges to use these commands.

```
                        REMOTE MAINTENANCE MENU

SRL              - Set Remote Line Loop Back
SRP              - Set Remote Payload Loop Back
SRDP<n>          - Set Remote Data Port Loop Back, n = 1 .. 4
RST1             - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1 ,0
S5C<n>           - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>           - Send 2047 Test Code in Data Port <n> Bit Stream
RTC              - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1 ,0
BT5<n>           - Activate BERT using 511 at Data Port n = 1 .. 4
BT2<n>           - Activate BERT using 2047 at Data Port n = 1 .. 4
```

Test code commands

BERT commands

Each test code is sent out framed. To set and reset test codes:

SQC	Send framed QRS code out the network interface.
S3C	Send framed 3-in-24 code out the network interface.
S1C	Send all 1s out the network interface. This may be required by the carrier.
S0C	Send all 0s out the network interface.
S2C1	Send 2047 code in the channels assigned to data port 1.
S5C1	Send 511 code in the channels assigned to data port 1.
RTC	Reset the test code generation.

To activate a BERT on the test codes:

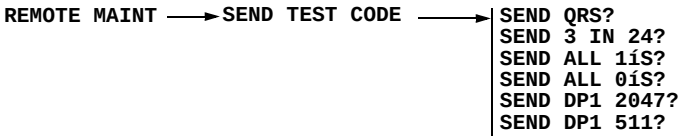
BTQ	Activate a BERT on QRS test code.
BT3	Activate a BERT on 3-in-24 test code.
BT1	Activate a BERT on all 1s test code.
BT0	Activate a BERT on all 0s test code.
BT51	Activate a BERT on 511 test code in channels assigned to data port 1.
BT21	Activate a BERT on 2047 test code in channels assigned to data port 1.

To deactivate or exit a BERT, enter Ctrl-C.

When you first activate a BERT, you will receive the message SEARCHING FOR PATTERN. When the DataSMART recognizes the test pattern, the BERT report will appear on the display.

Front-panel access

To set and reset test codes from the front panel, use these steps.



1 From REMOTE MAINT, push Next or Previous until SEND TEST CODE appears in the display. Push Select.

2 Push Next or Previous until the desired test code appears in the display.

3 Push Select to send the test code. You may receive one of the following responses:

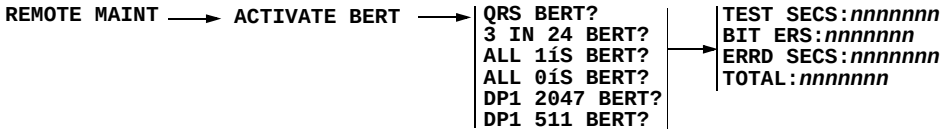
UNABLE TO SET — This means the DataSMART is not able to send the test code to the far-end device because another test condition exists.

NO CHAN ASSIGNED — This means the DataSMART is not able to send 2047 or 511 test code because the data port has no assigned channels.

4 After a few seconds, the message RESET TEST CODE appears. Push Select when you want to stop sending test code. You are asked to confirm the selection. You may receive the following response:

UNABLE TO CLEAR — The DataSMART is not able to reset the test code.

To activate a BERT, use the following steps. To deactivate a BERT, push Escape.



1 From REMOTE MAINT, push Next or Previous until ACTIVATE BERT appears in the display. Push Select.

2 Push Next or Previous until the desired BERT appears in the display.

3 Push Select to activate the BERT. The display will show SEARCHING, indicating that the DataSMART is searching for the specified test code in the incoming signal. When it finds it, the first readout in the list below appears. Push Next or Previous to see the other readouts. The readouts are updated dynamically as long as the BERT is active.

TEST SECS: *nnnnnnn* — The number of seconds, up to 65,535 maximum, since the test pattern was first detected.

BIT ERS: *nnnnnnn* — The number of bit errors, up to 65,535 maximum, that have occurred in the current second.

ERRD SECS: *nnnnnnn* — The number of errored seconds, up to 65,535 maximum, that have occurred since the DataSMART first detected the test pattern.

TOTAL: *nnnnnnn* — The total number of bit errors since the test code was first detected.

Setting a PING test

A PING request is used to test the connectivity of the network. PING sends a signal to a host or gateway, then listens for an echo response. The PING request is sent out the port which is specified by the NETIF command.

You set up a PING test by using the **ping** command in the Management Configuration menu. You must have super-user, configuration, or maintenance privileges.

```
                  MANAGEMENT CONFIGURATION MENU

TPW:<str>         - Set Telnet Password, str=0 to 15 characters
                    0 characters disables Telnet
NETIF:<p>         - Set IP Network Interface Paths
                    <c>, I = Inband, E = Ethernet, N = None, S = SLIP
SBTP:<m>          - Set BOOTP Mode.  <m> = F (First Start Up),
                    A (All Start Ups), D (Disabled)
IPR:<ipa>         - Set Default Route IP Address (N/A with In-Band)
IPA:<ipa>         - Set IP Addresses
IPM:<mask>        - Set IP Masks
                    <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
ping:[<vc>,<p>,]<ipa>,<n>,<l>
                  - Activate PING Test
                    <vc> = 1..1023
                    <p>  = D for data port, N for network (default = N)
                    <ipa>= IP address (xxx.xxx.xxx.xxx)
                    <n>  = number of PINGs to send 1..100
                    <l>  = payload 100..1000 bytes (default = 100)

AMC               - Advanced Management Configuration Menu
MCV               - View Management Configuration
```

The command syntax is:

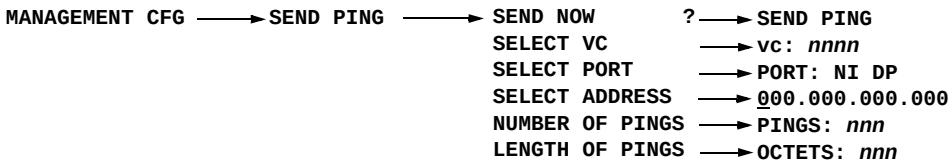
ping:*vc,p,ipa,n,l*

vc	Specify the virtual circuit. Enter a number between 1 and 1023.
p	Specify **D** to transmit the PING out the data port or **N** to send the PING out the network interface.
ipa	Specify the IP address of the required device.
t	Specify the time between PINGs.
l	Specify the length of the PING payload in octets. Enter a value between 100 and 1000. The default is 100.

To deactivate or exit a PING test, enter Ctrl-C.

Front panel access

To initiate a PING request from the front panel:



Configure your PING request, then push Select to activate the PING. The readouts are updated dynamically as long as the PING is active.

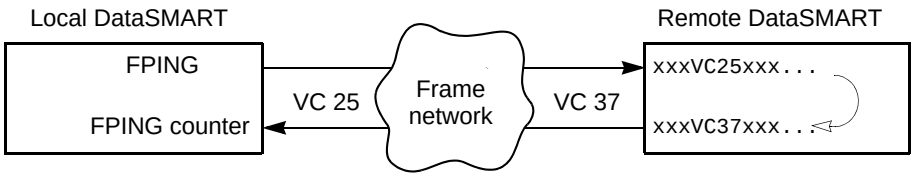
This information is also described in "Using PING to test network connectivity" on page 87.

Troubleshooting connection problems

Frame PINGs (FPINGs) provide a way for a frame monitoring DataSMART unit to test the virtual circuit (VC) connecting it to another frame monitoring DataSMART.

How FPINGs work

The local DataSMART sends an FPING message to a remote unit over a specified VC on a Frame Relay network. The FPING message includes a time stamp and the number of the VC. It is encapsulated as a frame packet so it can be routed through the Frame Relay network. The remote unit receives the FPING message. It replaces the VC number with the one it uses to connect to the local unit, adds its active IP address to the FPING message, and sends it back to the local unit. The local unit receives the echoed FPING message.



As soon as the FPING is received or is confirmed as lost, the local unit reports the FPING message's round-trip time in milliseconds and writes another line to the report or updates the front-panel display.

You can exit the FPING test by typing Ctrl-C.

```
RM> fptst 25,5

FPING Test on VC 25, 5 Second, 32 octet (^C to Terminate)

Current  Min  Max  Avg  # Lost  Total     Remote VC  Remote IP Address
-------  ---  ---  ---  ------  -----     ---------  -----------------
    100  100  100  100       0      1            37  192.92.340.1
    200  100  200  150       0      2            37  192.92.340.1
    300  100  300  200       0      3            37  192.92.340.1
    200  100  300  200       0      4            37  192.92.340.1
    200  100  300  200       1      5            37  192.92.340.1
```

Field	Description
CURRENT	The round-trip time in milliseconds, up to 2000, of the latest FPING message sent by this unit. A dash appears if the FPING was lost.
MIN	The shortest FPING round-trip time, in milliseconds, for this test.
MAX	The longest FPING round-trip time, in milliseconds, for this test.
AVG	The average FPING round-trip time, in milliseconds, for this test. (Lost FPING signals are not counted.)
# LOST	The number of FPING messages lost so far in this test.
TOTAL	The total number of FPING messages sent so far in this test.
Remote VC	The VC that the remote DataSMART uses to communicate with the local unit.
Remote IP Address	The active IP address of the remote DataSMART unit. This is usually the in-band IP address, but can be the SLIP IP address if the remote DataSMART unit hasn't yet been configured for in-band.

When you set up an FPING test, you specify:

- The virtual circuit ID you use to communicate with the remote unit
- The frequency of FPING messages (one message every specified number of seconds); the default is one FPING every 5 seconds
- The length of the FPING payload in octets (units of eight bits); the default is 32 octets

The frequency and length parameters are optional.

The FPING test is useful for testing an individual VC that you've just set up or on which you have detected problems. The DataSMART sends out FPINGs automatically on active VCs (see "About automatic Frame PINGs" on page 102). The FPING test does not interfere with automatic FPING generation.

Testing the DataSMART unit

In-band management and Frame PINGs (FPINGs) affect the count of octets transmitted and received by the unit. If you are measuring the DataSMART unit's performance in controlled conditions such as a laboratory test, you should disable in-band management (by setting **NETIF** to any value other than **I**) and disable FPINGs (with the **DFPO** command) before starting to test the unit.

Setting an FPING test

You set up a Frame PING test by using the **FPTST** command in the Frame Management Configuration menu. You must have super-user, configuration, or maintenance privileges.

```
                FRAME MANAGEMENT CONFIGURATION MENU

ESP/DSP             - Enable/Disable FRLM Spoofing
VCT:<vc>,<d>        - VC Termination
                      <vc> = 1..1023
                      <d>  = N(NI), D(DP), O(Off)
VCMOD:<vc>,<c>,<e> - Modify VC Monitoring Table
                      <vc> = 1..1023
                      <c>  = CIR 0..1536000 bits/sec
                      <e>  = EIR 0..1536000 bits/sec
FPTIM:<t>           - Set delay between Auto FPINGs
                      <t>  = 5...60 minutes
CIRTM:<t>           - Set time interval for CIR/EIR calculation
                      <t>  = 1...60 sec
FPTST:<vc>[,<p>[,<l>[,<t>]]]
                    - Activate FPING Test
                      <vc> = 1..1023
                      <p>  = D (Data Port), N (Network) (default = N)
                      <l>  = Payload 100..1400 bytes (default = 128)
                      <t>  = FPING frequency 5..255 secs (default = 5)
FMCV                - View Frame Configuration
```

The command syntax is:

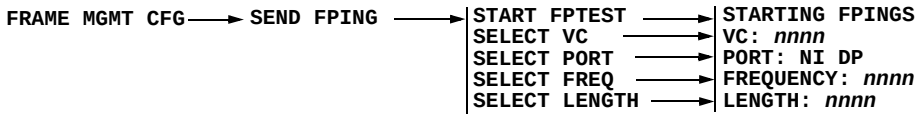
FPTST:*vc*,*p*,*l*,*t*

vc	Specify the virtual circuit. Enter a number between 0 and 1023.
p	Specify **D** for data port or **N** for network interface.
l	Specify the length of the FPING payload in octets. Enter a value between 0 and 1400. The default is 32.
t	Specify the time between FPINGs.

To deactivate or exit an FPING test, enter Ctrl-C.

Front-panel access

To set up a Frame PING test from the front panel:



When START FPTEST appears in the display, push Select to activate the FPING test. The display will show STARTING FPINGS, then the first readout in the list below appears. Push Next or Previous to see the other readouts. The readouts are updated dynamically as long as the FPING test is active.

CUR: *nnnn*	The round-trip time for the most recently sent FPING message in milliseconds, up to 2,000 maximum.
MIN: *nnnn*	The shortest round-trip time, in milliseconds, since the start of the test.
MAX: *nnnn*	The longest round-trip time, in milliseconds, since the start of the test.
AVG: *nnnn*	The average round-trip time, in milliseconds, since the start of the test. Lost messages are not counted.
LOST: *nnnn*	The number of FPING messages lost, since the start of the test.
TOTAL: *nnnn*	The total number of FPING messages sent since the start of the test.
RMT VC: *nnnn*	The virtual circuit ID used by the remote unit.
RMT IP: *nnn.nnn.nnn.nnn*	The active IP address used by the remote unit. This is usually the in-band IP address.

Push Escape to stop the FPING test. STOPPING FPINGS appears in the display, then SEND FPING.

CHAPTER

10 *Quick reference*

This chapter contains:

- A listing of all menus and commands available through the command-line interface
- A flowchart of all menus and commands available through the front-panel interface
- A description of how the DataSMART generates T1 alarms, based on signal conditions at the network interface
- A complete listing of the DataSMART specifications

Command-line menus and commands

The command-line interface provides menus that group the various commands by function and describe the use and syntax of each command.

To display a menu, simply enter the one- or two-letter acronym for the menu title.

Main Menu (MM)

```
        DataSMART 698 Version 1.00 Copyright (c) 1998 Kentrox
                      NAME: PORTLAND,OR

MM                      - Main Menu
SS                      - System Status
R                       - Reports Menu
RFRM                    - Frame Relay Monitoring Reports Menu

LM                      - Local Maintenance Menu
RM                      - Remote Maintenance Menu

AC                      - Alarm Configuration Menu
CC                      - Control Port Configuration Menu
DC                      - Data Port Configuration Menu
FC                      - Fractional T1 Configuration Menu
FMC                     - Frame Management Configuration Menu
MC                      - Management Configuration Menu
NC                      - NI Configuration Menu
PC                      - Password Entry and Configuration Menu
SC                      - System Configuration Menu
TC                      - TI Configuration Menu
^D                      - Logout
```

System Status (SS)

```
                  SYSTEM STATUS

ARC/DRC           - Access to/Disconnect from Remote Unit Control
S                 - System Status Screen Command

SSV               - View System Setup
```

Reports menu (R)

```
                  REPORTS MENU

UNSR / UNLR       - User NI Short/Long Performance Report
UTSR / UTLR       - User TI Short/Long Performance Report
FESR / FELR       - Far End PRM Short/Long Performance Report
NSR:[z]           - User NI Statistical Performance Report
TSR:[z]           - User TI Statistical Performance Report
                    z = Display Report, then Zero Counts (Optional)
AHR               - Alarm History Report
SHR               - Security History Report

PL:<len|style>    - Set Page Length, <len> = 20 .. 70 (or 0 = Off), or
                    <style> = P (Page Break), M (More), or V (View)
```

add/drop only

add/drop only

Frame Relay Monitoring Reports menu

```
                  FRAME RELAY MONITORING REPORTS MENU

NDSR[:z]          - NI/DP Statistical Report
VCSR[:<vc>[,z]] - VC Statistical Report
                    <vc> = 0..1023, * (All), or O (Other) (Optional)

VCUR[:<vc>[,z]] - VC Utilization Report
VCAR[:<vc>[,z]] - VC Availability Report
VCDR[:<vc>[,z]] - VC Delay Report
VCFR[:<vc>[,z]] - VC Frame Delivered Report
                    <vc> = 0..1023, or * (All) (Optional)

                    <z> = Display Report then Zero Counts (Optional)
```

Local Maintenance menu (LM)

```
                LOCAL MAINTENANCE MENU

SLL     - Set Line Loop Back
SPL     - Set Payload Loop Back
SLO     - Set Local Loop Back
STI     - Set TI Loop Back
SDP<n>  - Set Data Port Loop Back at Data Port, n=1
SDT<n>  - Set Data Terminal Loop Back at Data Port, n=1
RLB     - Reset Loop Backs

DST     - Do Self Test
```

add/drop only

Remote Maintenance menu (RM)

```
                REMOTE MAINTENANCE MENU

SRL             - Set Remote Line Loop Back
SRP             - Set Remote Payload Loop Back
SRDP<n>         - Set Remote Data Port Loop Back, n = 1
RST1            - Reset Remote Loop Back

SQC/S3C/S1C/S0C - Send Test Codes at NI: QRS, 3/24, 1, 0
S5C<n>          - Send 511 Test Code in Data Port <n> Bit Stream
S2C<n>          - Send 2047 Test Code in Data Port <n> Bit Stream
RTC             - Reset Test Codes

BTQ/BT3/BT1/BT0 - Activate BERT using Test Codes: QRS, 3/24, 1, 0
BT5<n>          - Activate BERT using 511 at Data Port n = 1
BT2<n>          - Activate BERT using 2047 at Data Port n = 1
```

Alarm Configuration menu (AC)

```
                ALARM CONFIGURATION MENU

EAM / DAM       - Enable/Disable Alarm Messages

EYL / DYL       - Enable/Disable YELLOW Activating an Alarm
DACT:<n>        - Alarm Deactivation time in seconds, n = 1..15
EST:<n>         - Errored Second Threshold, n = 0 .. 900
UST:<n>         - Unavailable Second Threshold, n = 0 .. 900
ST15/ ST60      - Set Threshold Timing to 15 or 60 Minutes

ACV             - View Alarm Configuration
```

Control Port Configuration menu (CC)

```
                CONTROL PORT CONFIGURATION MENU

EE / DE - Enable/Disable Character Echo

CCV     - View Control Port Configuration
```

Data Port Configuration menu (DC)

```
                DATA PORT CONFIGURATION MENU

EDI<n> / DDI<n> - Enable/Disable Data Inversion at Data Port, n=1

SCLK<n>:<clk>   - Source Clock at Data Port, n=1
                  clk = I (Internal), E (External)
TCLK<n>:<cmd>   - Transmit Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
RCLK<n>:<cmd>   - Receive Clock Inversion at Data Port, n=1
                  cmd = E (Enable), D (Disable)
DPLOS<n>:<los>  - LOS Input Signal at Data Port, n=1
                  los = R (RTS), D (DTR), B (Both), N (No Processing)

DCV             - View Data Port Configuration
```

Fractional T1 Configuration menu (FC)

```
                FRACTIONAL T1 CONFIGURATION MENU

<table>DP<port>:<rate>[,<nicn>]
                      - DP=Assign NI Channel Map for Data Port
    table A/B         - Tables A or B Containing Channel Assignment
    port  1           - Data Port Number
    rate  56/64       - Channel Rate in 1000 bps
    nicn  1 .. 24     - NI Channel numbers assigned to Data Port or
          1-24        - a contiguous range assigned.

<table>NI<nicn>:<ticn>,<nicn>:<ticn>, ...
                      - NI=Assign NI Channels to TI or IDLE
    table A/B         - Tables A or B Containing Channel Assignment
    nicn  1 .. 24     - NI Channel numbers
    ticn  V,D,I       - Voice/Data on TI Channel or I for Idle

CPAB / CPBA           - Copy A to B or B to A
LXA  / LXB            - Load and Execute Table A or B
TAV  / TBV            - View Table A or B
TXV                   - View Executing Channel Assignment
```

TI channel assignments available on add/drop units only

Frame Management Configuration menu (FMC)

```
                FRAME MANAGEMENT CONFIGURATION MENU

ESP/DSP             - Enable/Disable FRLM Spoofing
VCT:<vc>,<d>        - VC Termination
                      <vc> = 1..1023
                      <d>  = N(NI), D(DP), E(Either)
VCMOD:<vc>,<c>,<e> - Modify VC Monitoring Table
                      <vc> = 1..1023
                      <c>  = CIR 0..1536000 bits/sec
                      <e>  = EIR 0..1536000 bits/sec
FPTIM:<t>           - Set delay between Auto FPINGs
                      <t>  = 5...60 minutes
CIRTM:<t>           - Set time interval for CIR/EIR calculation
                      <t>  = 1...60 sec
FPTST:<vc>[,<p>[,<l>[,<t>]]]
                    - Activate FPING Test
                      <vc> = 1..1023
                      <p>  = D (Data Port), N (Network) (default = N)
                      <l>  = Payload 100..1400 bytes (default = 128)
                      <t>  = FPING frequency 5..255 secs (default = 5)
FMCV                - View Frame Configuration
```

Management Configuration menu (MC)

```
                MANAGEMENT CONFIGURATION MENU

TPW:<str>         - Set Telnet Password, str=0 to 15 characters
                    0 characters disables Telnet
NETIF:<p>         - Set IP Network Interface Paths
                    <c>, I = Inband, E = Ethernet, N = None, S = SLIP
SBTP:<m>          - Set BOOTP Mode.  <m> = F (First Start Up),
                    A (All Start Ups), D (Disabled)
IPR:<ipa>         - Set Default Route IP Address (N/A with In-Band)
IPA:<ipa          - Set IP Addresses
IPM:<mask>        - Set IP Masks
                    <ipa> and <mask> = n.n.n.n, n = 0 .. 255 (dec)
ping:[<vc>,<p>,]<ipa>,<n>,<l>
                  - Activate PING Test
                    <vc> = 1..1023
                    <p>  = D for data port, N for network (default = N)
                    <ipa>= IP address (xxx.xxx.xxx.xxx)
                    <n>  = number of PINGs to send 1..100
                    <l>  = payload 100..1000 bytes (default = 100)

AMC               - Advanced Management Configuration Menu
MCV               - View Management Configuration
```

Advanced Management Configuration menu (AMC)

```
                ADVANCED MANAGEMENT CONFIGURATION MENU

TCS:<str>           - Set SNMP Trap Comm String, str=1 to 15 characters
RCS:<str>           - Set SNMP Read Comm String, str=1 to 15 characters
WCS:<str>           - Set SNMP Write Comm String, str=1 to 15 characters

SSA:<p>             - Set Packet Screening via Source Address
                      p = I (IP Addr), N (None)
TRAP:<c>,<t>        - SNMP Trap Generation c = E (Enable), D (Disable)
                      t = S (Start), L (Link), A (Auth), E (Enterprise)
ADD:T,<ip>[<vc>,<p>]- Add IP Address to Trap Dest List
                      <vc> = Virtual Circuit, <p> = (N)I or (D)ata Port
                      <vc> and <p> are only required for In-Band
ADD:I,<ip>[,mask]   - Add IP Address to Screening List
DEL:<l>,<ip>        - Delete Address from Screening or Trap Dest Lists
                      <l> = I (IP Screen List), T (Trap Dest List)
                      <ip> and [mask] = n.n.n.n, n = 0 .. 255 (dec)
                      [mask] used only for IP Screen List and is optional

AMCV                - View Advanced Management Configuration
```

Network Interface Configuration menu (NC)

add/drop only

```
                 NI CONFIGURATION MENU

NSF/NESF/NERC    - NI SF/ESF/Ericsson Framing Format
NAMI / NB8       - NI AMI/B8ZS Line Coding
EPRM / DPRM      - Enable/Disable T1.403 PRM Generation out NI
FKA / UKA        - Framed(All 1ís)/Unframed (AIS) Keep Alive
EYEL / DYEL      - Enable/Disable YELLOW Activation out NI

              Line Build Out
NL0              -  0.0 dB
NL1              -  7.5 dB
NL2              - 15.0 dB

NCV              - View NI Configuration
```

Password Entry and Configuration menu (PC)

```
                 PASSWORD ENTRY AND CONFIGURATION MENU

EPS:<password>          - Enter Password
                          password = 6 to 12 characters

APS:<access>:<password> - Add Password
                          access   = SA - Super User
                                     CA - Configuration
                                     MA - Maintenance
                          password = 6 to 12 characters

DPS:<password>          - Delete Password
                          password = 6 to 12 characters, or * for all

PUV                     - View User Access Privilege
PCV                     - View Password Configuration
```

System Configuration menu (SC)

```
                SYSTEM CONFIGURATION MENU

SD:<mm>,<dd>,<yy>   - Set Date (Warning: This also clears reports)
ST:<hh>,<mm>        - Set Time (Warning: This also clears reports)
SN:<id>             - Set Name
SMT/SMM             - Mode = Transparent/Monitor
EFP / DFP           - Enable/Disable Front Panel Operation
CLK:<src>           - Clock Source, src = L (Loop), I (Internal)
                      T (TI Rcv)
ALGOUT:<n>          - Autologout, n = 0..60 minutes
ZALL                - Zero All Counters used in User Reports
TSWDL:<i>           - Download program from a file via TFTP
                      i = n.n.n.n, n = 0..255 (dec), the
                          IP address of the TFTP host system
BOOT                - Re-boot the system
WYV                 - View "What's Your Version" Information
RSD                 - Reset System to Default Values
SCV                 - View System Configuration
```

T option available on add/drop only

Terminal Interface Configuration menu (TC)

```
                  TI CONFIGURATION MENU

TSF/TESF/TERC  - TI SF/ESF/Ericsson Framing Format
TAMI/TB8       - TI AMI/B8ZS Line Coding
TIDL:<c>       - Idle Code, c = 00-FF Hex

                  TI Equalization
TE0            -   0 - 133 ft
TE1            - 133 - 266 ft
TE2            - 266 - 399 ft
TE3            - 399 - 533 ft
TE4            - 533 - 655 ft

TCV            - View TI Configuration
```

Front-panel menus and commands

In the flowcharts below, movement through the front-panel interface is denoted as follows:

- A vertical line to the left of a column represents a menu listing that you cycle through by pushing the Next or Previous button.
- A vertical line to the right of a column means that each item in the list has the same entry path into the next menu or command (listed to the left).
- An arrow represents a path you enter by pushing the Select button, and exit by pushing the Escape button.
- Bold face type represents a specific path through the interface, starting at the top of the menu hierarchy.

You cycle through command fields by pushing the Next or Previous button. You select field values by pushing the Select button.

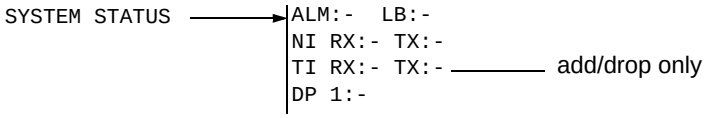
You can always return to the top menu by pushing the Escape button repeatedly.

If the front-panel is disabled, it defaults to a display of %EFS (percentage error-free seconds).

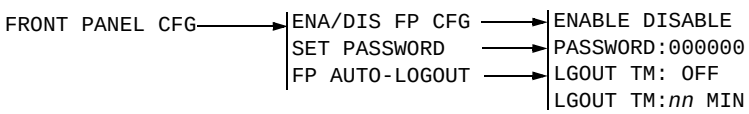
Top level menu

```
SYSTEM STATUS
FRONT PANEL CFG
T1 REPORTS
FR REPORTS
ALARM CFG
CONTROL PORT CFG
DATA PORT CFG
FRACTIONL T1 CFG
FRAME MGMT CFG
SYSTEM CFG
TERMINAL CFG
NETWORK CFG
MANAGEMENT CFG
ADVNCD MGMT CFG
REMOTE MAINT
LOCAL MAINT
```

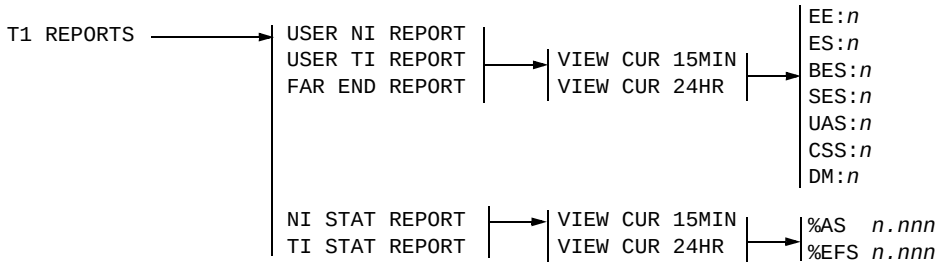
System status



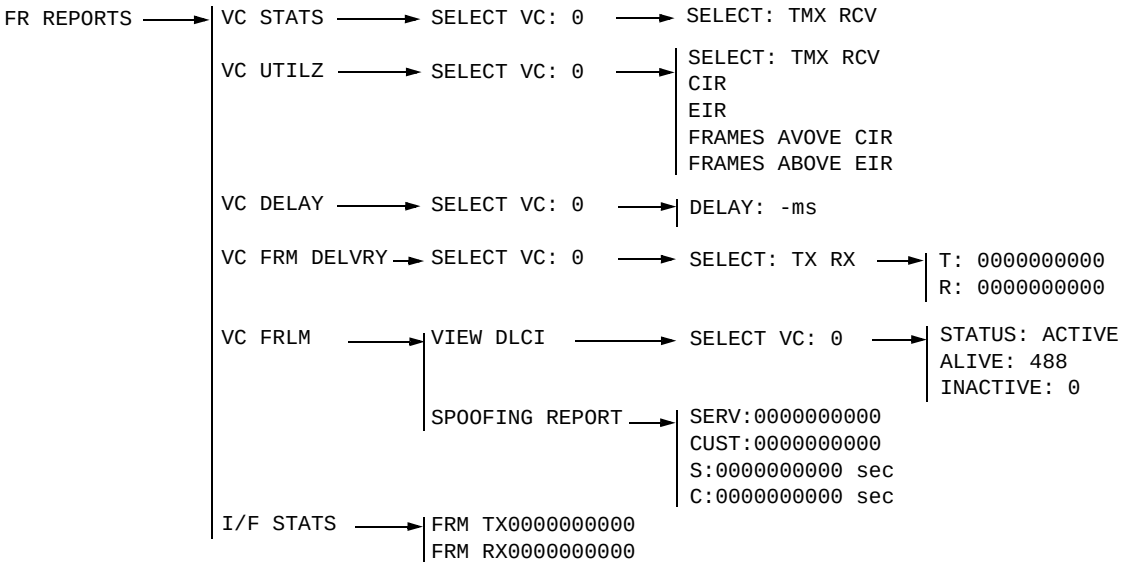
Front-panel configuration



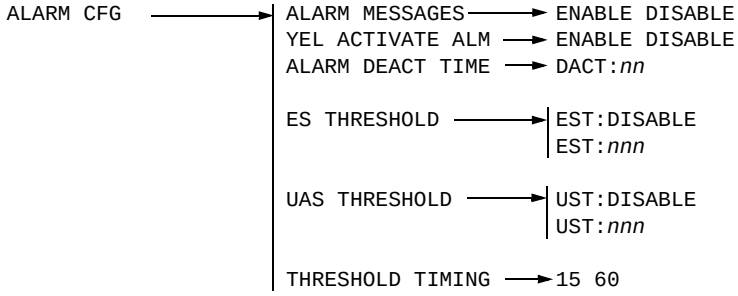
T1 Reports



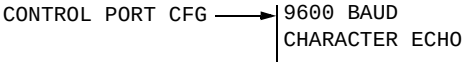
Frame Reports



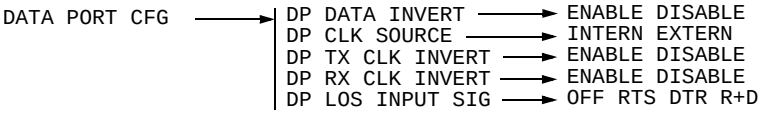
Alarm configuration



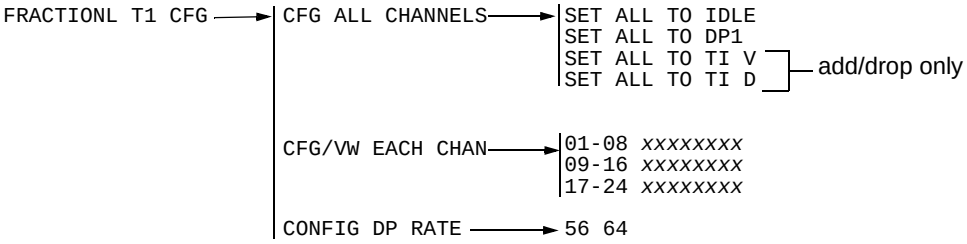
Control port configuration



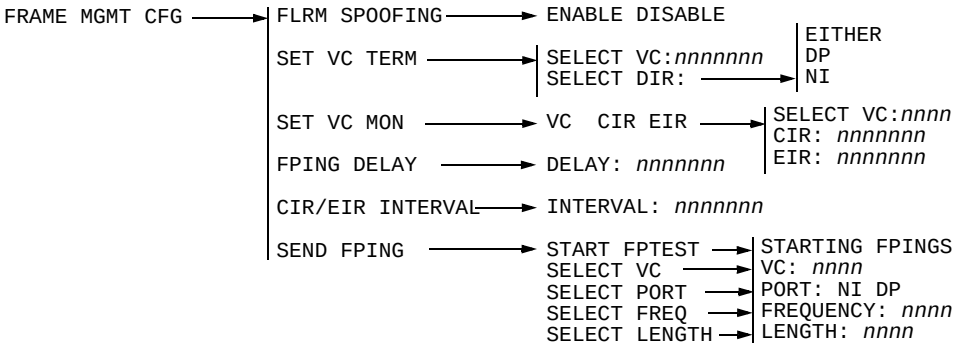
Data port configuration



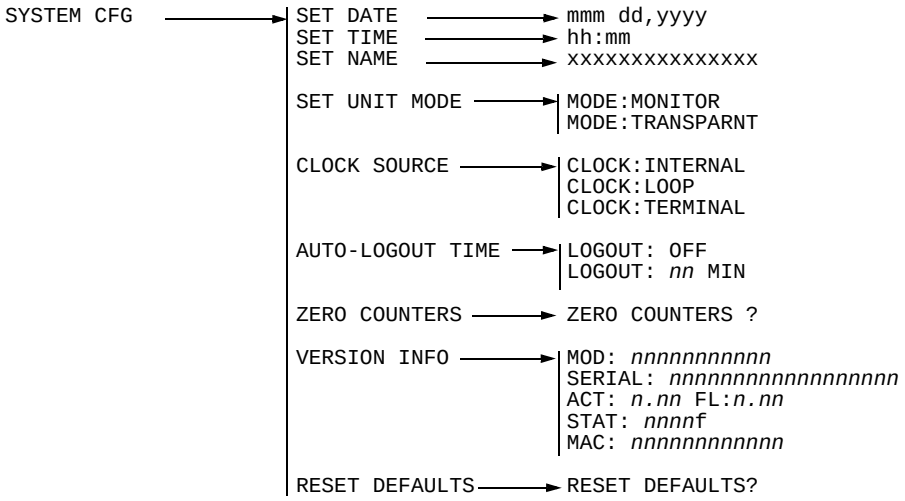
Fractional T1 configuration



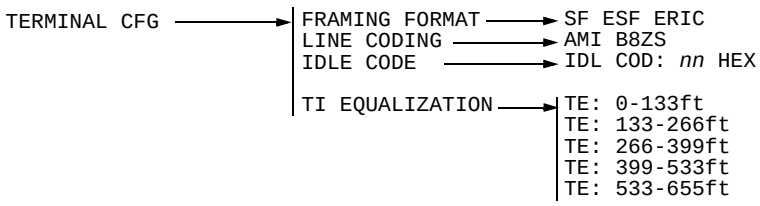
Frame Management configuration



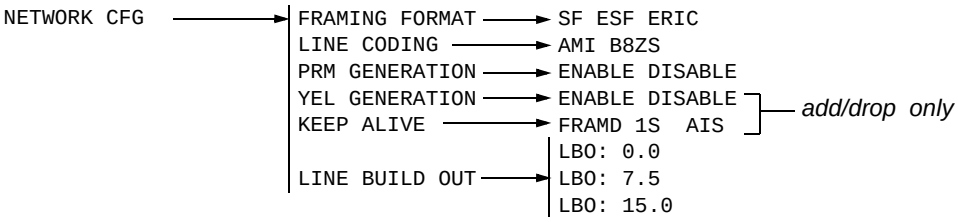
System configuration



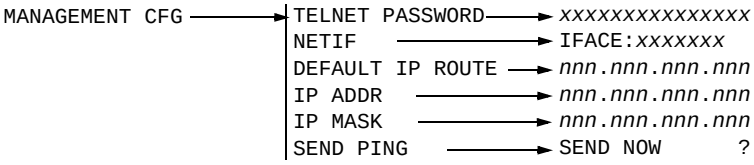
Terminal configuration (DataSMART 698 only)



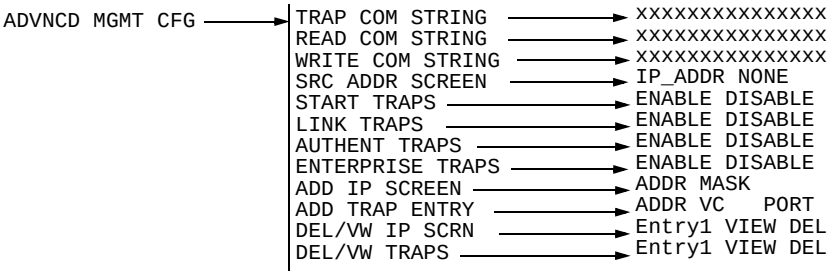
Network configuration



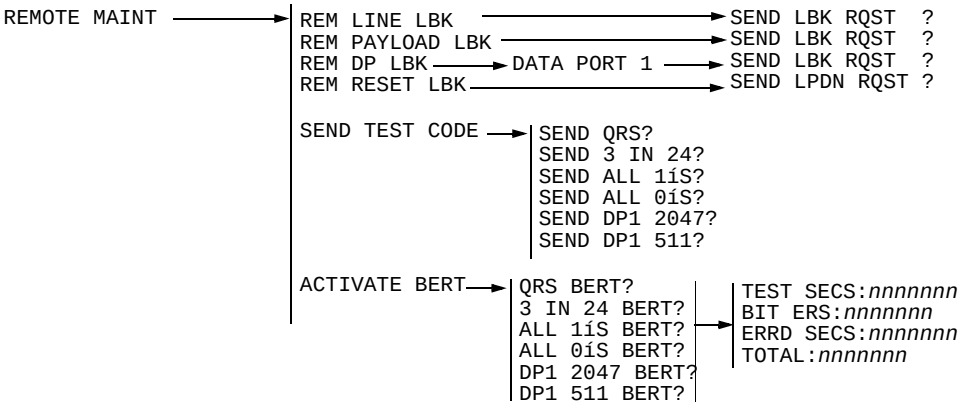
Management configuration



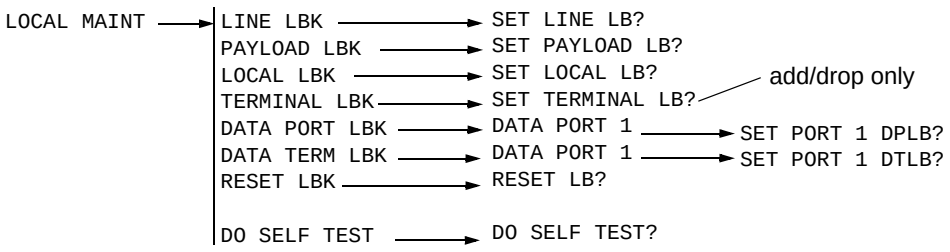
Advanced management configuration



Remote maintenance



Local maintenance



T1 alarms and signal processing

This section describes how the DataSMART transitions into and out of an alarm state. It also describes in detail the alarms that can occur at the network and terminal T1 interfaces and the signal conditions that cause them.

NOTE
For a complete listing of all alarms generated by the DataSMART and appropriate troubleshooting procedures, refer to Chapter 9, "Troubleshooting".

What happens when alarms occur

When the DataSmart transitions to an alarm state, it performs various actions:

- It illuminates appropriate LEDs on the front panel.
- It updates the System Status display with status information about the alarms and signal conditions at the network interface, terminal interface, and data ports.
- It outputs an SNMP trap or an alarm message to the control device (if traps or messages are enabled) and logs the alarm message in the Alarm History report.
- It transmits yellow alarms and idle code out the interfaces and data ports as appropriate.
- It switches the clock source to internal master timing, if the condition obstructs the clocking source.

How alarms are generated

The DataSMART generates alarms based on error events that occur on an input signal. Error events are also referred to as signal conditions. For instance, a loss of signal event (LOS) is also referred to as an LOS signal condition. A signal condition is a current, instantaneous status of the received signal at the interface. The signal condition may persist, may be intermittent, or may disappear immediately.

If a signal condition persists or is intermittent but frequent, the DataSMART transitions into an alarm state, a process called "alarm integration." The algorithm that controls alarm integration is designed to prevent alarms from being raised every time a signal condition occurs briefly, and to prevent the alarm from being deactivated every time the signal condition temporarily flickers off.

The alarm integration algorithm

The alarm integration algorithm uses two values: the alarm integration time and the decay rate. (On the DataSMART the alarm integration time is set to 2.5 seconds and the decay rate is 1/5.)

The algorithm maintains a count for each signal condition. Whenever a signal condition exists, time accrues to the count for that signal condition. For instance, if the OOF signal condition exists for 1 second, 1 second is accrued to the OOF count. Time spent out of the signal condition is multiplied by 1/5 (the decay rate) and subtracted from the count, which has a minimum value of 0. When the count exceeds 2.5 (the alarm integration time), the transition to an alarm state occurs.

The alarm integration algorithm is defined in detail in AT&T 62411.

Transitioning out of the alarm state

When a signal condition that has produced an alarm goes away, the alarm persists until the condition has been absent for a period of time referred to as the alarm deactivation time. The alarm deactivation time is user-configurable and by default is 15 seconds. (See "Setting the alarm deactivation time" on page 49 for more information.)

Alarm reporting

The DataSMART produces an alarm message each time a line transitions to a new alarm state. The "CLR" message is not sent until all alarms on a particular interface clear. All alarm messages are output to the device connected to the control port and are logged in the Alarm History report. To see the Alarm History report, type **AHR** at the command line.

You can examine the current status and track the changing conditions on an interface using the System Status report (type **S** at the command line). This report shows the current alarm state of the DataSMART as well as the signal condition of the input and output signal at all interfaces. The status report is updated once a second upon any changes to the alarm state or signal conditions. You can also track system status from the LCD display on the front panel of the DataSMART. See "Examining system status" on page 139 for more information.

A received T1 signal is classified as being in one and only one alarm state at a time. Alarm states have a priority. If the signal satisfies more than one of the requirements for an alarm state, the higher priority alarm applies. Because of this, and because of the deactivation delay of an alarm, the System Status report could contain an entry in which an interface is in an alarm state that does not match the signal condition.

For example, suppose the alarm deactivation time period is set to 15 seconds, and suppose the signal condition for the NI received signal is AIS. After the alarm integration requirements are met, the line is declared to be in the AIS alarm state. Now suppose that the signal condition changes from AIS to OOF. At this point the DataSMART will add a new entry to the status report to show the change in the signal condition. However, in that same entry, the alarm condition will be shown as AIS because the alarm deactivation time period has not passed.

Now assume the OOF condition persists for 2.5 seconds, and thus has satisfied the conditions for alarm integration. Because the OOF has a lower priority, and because of the 15-second deactivation period for alarms, the alarm state will still be AIS. However, once the 15 seconds have passed, the alarm state will transition from AIS to OOF, and the DataSMART will add a new entry to the status report.

Signal conditions

The table below lists the signal conditions for the DataSMART in priority order, highest priority first. A received T1 signal can be in one and only one of the signal conditions at a time.

Condition	Definition
LOS	Loss of Signal. No pulses are being received. The LOS signal condition starts upon receipt of 192 consecutive spaces or zeros. The LOS signal condition clears when the signal contains 32 consecutive bits with at least 4 ones and no more than 15 consecutive zeros.
AIS	Alarm Indication Signal. A signal with a 99.9% ones density for a minimum of 3 milliseconds and no framing detected is being received. The AIS condition is detected in the presence of a 1×10^{-3} bit error rate. An AIS condition is declared when both out-of-frame and all 1s conditions are present at the interface. The AIS condition clears when either the OOF, all 1s, or both conditions clear.
OOF	Out of Frame. The received signal does not contain a T1 framing pattern. The OOF signal condition is declared when two out of four frame bits are in error (SF and Ericsson framing) or when two out of six frame bits are in error (ESF framing). The OOF signal condition clears when a reframe occurs.
EER	Excessive Error Rate. A framed T1 signal with an event error rate exceeding the user-supplied threshold is being received. This condition clears when the next time interval's error count is less than the threshold.
YELLOW	The received signal contains the yellow alarm pattern in bit two of each DS0 (SF framing) or a yellow alarm code word in the ESF Data Link (ESF framing). The condition clears when the yellow alarm pattern is no longer detected in the received signal.
Good Signal	A framed T1 signal with none of the above listed signal conditions.

Alarms

For each of the signal conditions described in the previous table there is an alarm state. The table below lists the T1 alarms for the DataSMART in priority order, highest priority first. Note that, as shown in the table, not all alarms use the alarm integration algorithm described on page 177.

Alarm	Definition
LOS	The LOS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the LOS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent LOS signal condition). The LOS alarm clears after a continuous time period of *n* seconds with no LOS signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
AIS	The AIS alarm starts upon a total of 2.5 seconds of alarm integration time spent in the AIS signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent AIS signal condition). The AIS alarm clears after a continuous time period of *n* seconds with no AIS signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
OOF	The OOF alarm starts upon a total of 2.5 seconds of alarm integration time spent in the OOF signal condition (the alarm integration time has a decay rate of 1/5 in case of an intermittent OOF signal condition). The OOF alarm clears after a continuous time period of *n* seconds with no OOF signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
Yellow Alarm	The yellow signal alarm is declared after receiving the yellow signal for 1 second. Once declared, the alarm stays active for a minimum of one second. It is cleared upon detection of an input signal without the yellow alarm pattern present.
EER	The EER alarm starts immediately upon entering the EER signal condition. The EER alarm clears after a continuous time period of *n* seconds with no EER signal condition, where *n* is the alarm deactivation time period set by the user via the DACT command.
Clear	None of the above listed alarms is active.

Specifications

Table 10—Environmental specifications

	Parameter	Specification
Temperature	Storage	-20°C to 66°C (5% to 65% RH)
	Operating	0°C to 50°C[1] (5% to 90% RH, noncondensing)
Powering	AC input range	90 to 130 VAC, 47 to 63 Hz
	Power interruptions	Loss of power does not damage the unit nor change the configuration settings.

[1] At about 40° C (104° F), the LCD darkens and becomes difficult to read. The rest of the unit remains operable to 50° C (122° F).

Table 11—Physical specifications

	Parameter	Specification
	Size with feet	1.7 in. x 7.75 in. x 11.5 in.
	Size without feet	1.65 in. x 7.75 in. x 11.5 in.
	Weight	Approximately 2.5 lb.

Table 12—Serial control port specification

	Parameter	Specification
Connector	DTE	DB9P
	Baud rate	9600
	Electrical interface	EIA-574

Table 13—Data port interface specifications

	Parameter	Specification
	Bit rates	56 kHz to 1536 kHz
	Connector	34-pin MRAC34S connector
	Electrical interfaces	V.35 compatible
	Interface type	DCE

Table 14—Electrical interface specifications - network interface

	Parameter	Specification
Common	Line rate	Internal or external clock; 1.544 Mbps ± 32 ppm When timing is derived from input signal: 1.544 Mbps ± 200 bps. Output line rate follows input line rate.
	Line code	AMI or B8ZS (selectable)
	Line impedance	100 ohms ± 10 ohms at 772 kHz 100 ohms ± 20% over the frequency band 100 kHz to 1Mhz
	Lightning protection	Lightning surges defined per FCC Part 68 shall not damage the unit.
	Framing format	SF or ESF per ANSI T1.403-1989 Ericsson Framing (defined as valid F_T bits only)
Input Only	Input level	DSX-1 to -27.5 dB
	Input jitter tolerance	Per TR 62411-1990 (p. 4.7.1)
Output Only	Output level	Per ANSI T1.403-1989 3.0 Volt peak ± 10% into 100 ohms at output connector
	Output signal	Tolerant to impedance mismatches
	Line build out	0, 7.5, 15.0 selectable
	Output jitter	TR 62411-1990 (p 4.7.2)
	Jitter transfer	DSU: TR 62411-1990 (p 4.7.3)
	Pulse density	> 12.5% (when enabled)

Table 15—Electrical interface specifications - terminal interface

	Parameter	Specification
Common	Line rate	Internal; 1.544 Mbps ± 32 ppm When timing is derived from input signal: 1.544 Mbps ± 200 bps. Output line rate follows input line rate.
	Line code	AMI or B8ZS (selectable)
	Line impedance	100 ohms ± 10 ohms at 772 kHz 100 ohms ± 20% over the frequency band 100 kHz to 1Mhz
	Framing format	SF or ESF per ANSI T1.403-1989 Ericsson Framing (defined as valid F_T bits only)
Input Only	Input level	DSX-1 to -10.0 dB
	Input jitter tolerance	Per TR 62411-1990 (p. 4.7.1)
	Input jitter transfer	Per TR 62411-1990 (p. 4.7.2)
Output Only	Output level	DSX-1 at connector (no equalization enabled)
	Equalization	Up to 655 feet selectable, 5 steps

Table 16—Compatibility

Standard
AT&T TR54019 Appendix A (Fractional T1)
EIA T1.403/1995
TIA-547

Table 17—Supported loopbacks

Loopback	Definition
LLB Line loopback	A minimum penetration loopback at the NI interface.
PLB Payload loopback	An interior loopback, looping the payload back to the NI.
DPLB Data Port loopback	Looping the bit stream assigned to the data port back towards the NI.
DTLB Data Terminal loopback	Looping the bit stream back to the data terminal equipment connected to the data port.
LOC Local loopback	An interior loopback, looping only the payload back to the terminal interface or data ports.
TILB Terminal Interface loopback	A minimum penetration loopback at the terminal interface.

Pinouts

For connection to T1 network: Use AT&T Type ABAM cable or equivalent (individually-shielded twisted pair, rated at 100 ohms at 1 MHz).

RJ48C

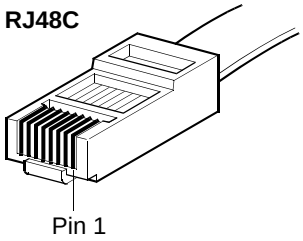


Table 18—Network interface pinout for the 8-pin RJ48C connector

Pin number	Circuit name
1	RxD data (T1)
2	RxD data (R1)
4	TxD data (T)
5	TxD data (R)
7, 8	No connection
3, 6	No connection

Table 19—Terminal interface pinout for the 8-pin RJ48C connector

Pin number	Circuit name
1	RxD data (T)
2	RxD data (R)
4	TxD data (T1)
5	TxD data (R1)
3, 6	No connection

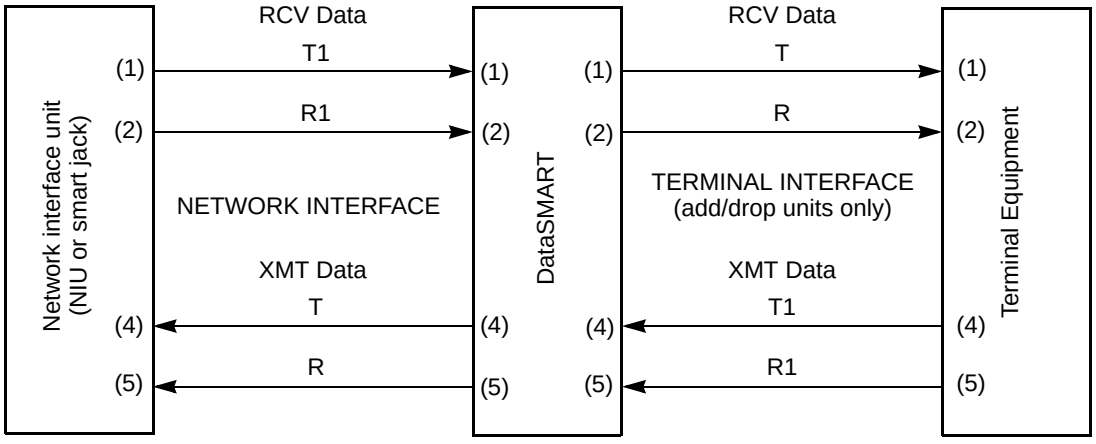


Table 20—9-pin DE9S (DCE)

Signal	DE9 Pin Number	DB25 Equivalent	Direction
Rec Sig Det	1	8	OUTPUT
Received Data	2	3	OUTPUT
Transmit Data	3	2	INPUT
DTE Ready (DTR)	4	20	INPUT
Signal Ground	5	7	—
Data Set Ready (DSR)	6	6	OUTPUT
Request to Send (RTS)	7	4	INPUT
Clear to Send (CTS)	8	5	OUTPUT
Not Used	9	None	—

Table 21—Ethernet 10Base-T pinout

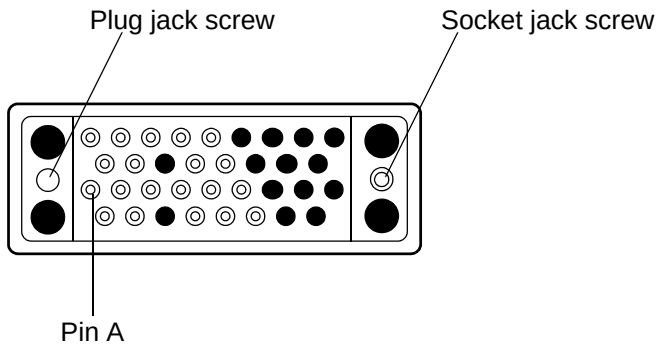
Pin Number	Signal
1	TD+
2	TD-
3	RD+
6	RD-
4	Not used
5	Not used
7	Not used
8	Not used

The following table shows V.35 pin assignments for the data port socket. Pin identifiers (A, B, etc.) appear on the plug and socket.

Table 22—V.35 connector pin assignments for data port

Pin	Designator ITU/EIA	Circuit Name	Source
A		Shield	
B	102/AB	AB, Signal Ground	
C	(a) 105/CA	CA (A), RTS	DTE
D	(a) 106/CB	CB (A), CTS	DCE
E	(a) 107/CC	CC (A), DSR	DCE
F	(a) 109/CF	CF (A), Received Line Signal Detector (DCD)	DCE
H	(a) 108.2/CD	CD (A), DTR	DTE
K		Local Data Terminal Loopback	DTE
L		Local Data Terminal Loopback	DTE
P	(a) 103/BA	BA (A), Transmitted Data A	DTE
S	(b) 103/BA	BA (B), Transmitted Data B	DTE
R	(a) 104/BB	BB (A), Received Data A	DCE
T	(b) 104/BB	BB (B), Received Data B	DCE
U	(a) 113/DA	DA (A), External Clock	DTE
W	(b) 113/DA	DA (B), External Clock	DTE
V	(a) 115/DD	DD (A), Receiver Signal Element Timing	DCE
X	(b) 115/DD	DD (B), Receiver Signal Element Timing	DCE
Y	(a) 114/DB	DB (A), Transmit Signal Element Timing	DCE
AA	(b) 114/DB	DB (B), Transmit Signal Element Timing	DCE

Figure 15—DataSMART 696 V.35 data port jack



Index

Symbols

A

B

C

D

E

U

V

Y

Z